

DAS WIRTSCHAFTSMAGAZIN ZUR DIGITALISIERUNG

DIGITALE WELT

ZUKUNFT | EINFACH | ENTDECKEN

Ausgabe 3 • Juli • August • September • 2018

IoT – Strategien zur digitalen Vernetzung

62 Seiten
Experten-
beiträge
zu IoT

Use Cases

IoT in der Anwendung:
von Business IoT bis Industrial IoT

Praxiskonzepte

Datenmanagement für IoT und
Auswirkungen der Vernetzung

Sicherheit

Herausforderungen und
Lösungen für die sichere Anwendung

INTERNET OF THINGS

Realer Hype oder eine neue Blase?
Vernetzt denken und handeln



Der Universitätsprofessor
über Roboterforschung und
deren Zukunft

Sami Haddadin

Connecting Global Competence



The Leading Summit for Cyber Security

Cybersicherheit aus einer ganz neuen Perspektive – Tauschen Sie sich in diesem einzigartigen Veranstaltungsformat mit internationalen Entscheidern und Experten aus.

**Machen Sie Cyber Security zum
Wachstumshebel für Ihr Unternehmen!**

20. – 22. September 2018
ICM – Internationales
Congress Center München

cmdctrl.com

CMD CTRL

Command Control
Munich 2018

DIGITALE WELT AUSGABE 3 | 2018



12

VERY DIGITAL PERSON
Sami Haddadin

24

INTERNET OF THINGS
Realer Hype oder
eine neue Blase?

DIGITALER MARKTPLATZ

- 9 **News & Trends** | Kurioses und Innovatives
- 10 **Digitalisierung in Zahlen** | Fakten, die überraschen

HINTER DEN KULISSEN

- 16 **Messe München** | Der gekonnte Mix aus digital und real

VERY DIGITAL PERSON

- 12 **Sami Haddadin** | Über Roboterforschung und deren Zukunft

24 WISSEN – IoT

ALLGEMEIN

- 26 **Donald Wachs** | IoT – realer Hype oder eine neue Blase?
- 28 **Dr. Nils Daecke** | Internet of Things – Game Changer oder Gadget?
- 30 **Axel Godoy** | Sind deutsche Unternehmen bereit für IoT?
- 32 **Felix Heimbrecht** | IoT und AI: eine Co-Evolution
- 34 **Dr. Thomas Zander** | „Industrial Internet of Things“-Lösungen helfen uns allen – wenn die Anbieter ihre Hausaufgaben machen
- 35 **Harald A. Summa** | Die drei Ausprägungen des IoT und was wir dafür tun können, dass unsere digitale Zukunft eine gute Zukunft wird
- 37 **Christoph Henkels** | NarrowBand IoT – der schlanke Einstieg ins Internet der Dinge

- 39 **Andreas Odenkirchen** | Industrial Internet of Things (IIoT): Darauf kommt es an
- 41 **Klaus Jaworski** | Virtual Reality – Science Fiction von heute
- 42 **Sascha Hellermann** | Mit Blockchain-Technologie bereit für das Internet of Things
- 43 **Dr. Thomas Endres** | IoT – eine große Chance für Europa
- 45 **Georg Goller** | Der Weg zur digitalen Transformation
- 46 **Michaela Tiedemann** | Warum künstliche Intelligenz dem Internet of Things zum Durchbruch verhelfen wird

SICHERHEIT

- 47 **Markus Reiniger** | Internet of Things (IoT) – von der Zukunft von Endgeräten bis hin zu ihren Sicherheitsproblemen
- 49 **Nigel Stanley** | IoT-Geräte: Wenn Cyber Security für Kunde und Marke zum kritischen Faktor wird
- 50 **Claus Vaupel** | Sicherheitsrisiko Internet of Things
- 51 **Nicolas Ehrschwendner** | Datenverlust lauert auch im IoT
- 52 **Jan Junker** | Hackers Paradise – Sicherheit im Internet of Things
- 53 **Claas Lorenz** | IoT: Risikomanagement nur mit Security by Design
- 54 **Wilfried Kirsch** | Internet der Dinge: Security Guidelines



16 HINTER DEN KULISSEN
Messe München – der gekonnte
Mix aus digital und real



86 SZENE
München, Düsseldorf
und Leipzig

DIGITALE VERNETZUNG

- 56 **Robert Romanski** | Datenexplosion: wirtschaftliches Management und Hochverfügbarkeit dank Hyperscale-Rechenzentren
- 57 **Carsten Hochschon** | Datenübertragung mittels Blockchain
- 59 **Dr.-Ing. Darko Sucic** | Vernetzt denken und handeln
- 60 **Jochen Busch** | Ein neues Netz als Herzstück für intelligente Städte
- 61 **Florian Hermsdorf** | Das Internet wird unsichtbar
- 62 **Henning Neu** | I(di)oT – wie Smart Devices unserer Gesellschaft Innovation vorgaukeln und unseren Alltag komplexer machen
- 64 **Manfred Klaus** | Warum das „Internet der Dinge“ in den Marketingplan gehört
- 65 **Alexander Eser** | Internet of Things (IoT) und unser Zuhause – durch Artificial Intelligence (AI) wird der Zero Click Sale möglich
- 67 **Kurt Kapp** | IoT – neue Handlungsfelder für die Landeshauptstadt München
- 69 **Markus Reichenberger** | IoT im Zusammenhang von Interoperabilität, Echtzeitanwendungen, Architekturen und sozialer Akzeptanz
- IOT IN DER PRAXIS**
- 71 **Dr. Thomas Lücking** | Vom Produkt zum Service – organisatorischer Wandel als Voraussetzung für erfolgreiche IoT-Lösungen
- 74 **Hanna Pradler** | Wie IoT-Geräte für Konsumenten nützlicher werden
- 75 **Math Huntjens** | Die smarte Brücke zwischen Produktion und Office
- 76 **Christian Haas** | Am Ende gewinnt immer der Kunde ...
- 77 **Steffen Krotzsch** | Das Internet der Dinge im Versicherungsbereich

- 78 **Dr. Andreas Leupold** | Industrial Internet of Things (IIoT): rechtlicher Handlungsbedarf für Unternehmen
- 80 **Falk Senger** | IoT-Plattformen sind Voraussetzung für Industrie 4.0
- 82 **Uwe Weber** | Industrial Internet of Things: wie der Fertigungsablauf mittels Edge Computing intelligent gesteuert wird
- 83 **Tim Kappler** | Die flächendeckende Anwendung von IoT-Geräten in Industrie-Unternehmen – eine Bestandsaufnahme aus Sicht der Rückversicherung

SZENE

- 86 **München** | Digitale Stadt München e. V.
- 87 **Düsseldorf** | Digitale Stadt Düsseldorf e. V.
- 88 **Leipzig** | XPOMET

KOLUMNEN

- 15 **Petra Bernatzeder** | Ist das schon Burnout?
- 23 **Marcus Raitner** | Organisationsrebell: Veränderung braucht Störung
- 85 **Uwe Walter** | Nutzen Sie Storytelling – die fünf Storys, die jeder braucht

IMMER DABEI

- 7 **Editorial** | Frank Schmidt
- 89 **Fachbeirat**
- 89 **Impressum**
- 90 **Termine**

Die nächste
DIGITALE WELT
erscheint am
05.09.2018

Titel: iStock.com/Rost-9D, Ansgar Pudenz, Fotos: iStock.com/Rost-9D, Leibniz Universität Hannover, Messe München, Digitale Stadt Düsseldorf e.V.

DIGICON 2018

DIGITALE WELT CONVENTION

21. UND 22. NOVEMBER 2018

Palais Lenbach, München



Thema:

MACHINE LEARNING – IMPULSE DURCH QUANTEN COMPUTING, DATA MINING UND REINFORCEMENT LEARNING

Heute lernen, die Zukunft zu gestalten.

AUSZUG UNSERER HOCHKARÄTIGEN REFERENTEN



Prof. Dr. Claudia Linnhoff-Popien
LMU München
Digitale Stadt München e. V.



Prof. Dr. Fredmund Malik
CEO & Erfolgsautor
Malik Institute for Complexity and Management



Prof. Dr. Katharina Morik
Lehrstuhl für künstliche
Intelligenz
TU Dortmund



Dr. Jörg Ochs
Geschäftsführer
SWM Infrastruktur
Verwaltung GmbH



Thomas Schlereth
Geschäftsführer
Can Do GmbH



Dr. Roland Schütz
EVP and CIO
Lufthansa Group Airlines
and Digital Initiatives



Prof. Dr. Patrick van der Smagt
Director AI Research
VW Group



Dr. Heiko Udluft
Data Scientist &
Tech-Team Lead
Airbus



Dr. Johannes Wechsler
CIO
ProSiebenSat.1 Media SE

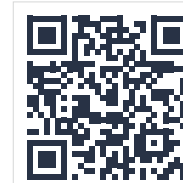
JETZT ANMELDEN!

EARLY BIRD
25 % Rabatt
bis 30. Juni 2018

LAST CALL
15 % Rabatt
bis 14. September 2018

EXKLUSIVER DIGITALE WELT RABATT

mit einem zusätzlichen Nachlass von 10 %
Ihr Code: DIGITALEWELT10



Für Ihre Anmeldung sowie
weitere Informationen gehen
Sie bitte auf unsere Webseite
www.digitaleweltmagazin.de/digicon

Unsere Sponsoren und Partner



CALL FOR CONTRIBUTION

für den
DIGITALE WELT Blog

Platzieren Sie Ihre Digitalthemen von morgen auf der Plattform von heute mit bislang über 147.000* Beitragsaufrufen:
digitaleweltmagazin.de/blog

Werden Sie Autor!

Ihre Vorteile im Überblick:

- ✓ Teilen Ihres Fachwissens mit einer breiten digitalen Leserschaft
- ✓ Potentielle Veröffentlichung im **DIGITALE WELT** Printmagazin
- ✓ Bekanntheitssteigerung Ihres Unternehmens
Mediale Positionierung von gezielten, für Sie relevanten Digitalthemen
- ✓ Aktive Beteiligung am aktuellen Dialog zur Digitalisierung
- ✓ Multiplier Effekt durch die Verbreitung über Social Media
- ✓ Profilschärfung und Positionierung gezielter Unternehmensvertreter

Aktuelle Blog-Rubriken:

Blockchain, Cyber Security, Affective Computing, Internet of Things, Machine Learning, u.v.a.m.



DR.-ING. FRANK SCHMIDT

Dr.-Ing. Frank Schmidt ist Executive Vice President Engineering der Bosch Engineering GmbH, einer 100-prozentigen Tochtergesellschaft der Robert Bosch GmbH. Er studierte Elektrotechnik an der Universität Kaiserslautern, wo er 1996 auch seine Promotion abschloss. Seit 1996 hat er in der Bosch-Gruppe verschiedene Stationen durchlaufen und ist seit 2016 Geschäftsführer Entwicklung der Bosch Engineering GmbH. Mit seiner langjährigen Expertise treibt er den Entwicklungsbereich voran und ist gefragter Redner bei Kongressen. Die Bosch Engineering bietet seit 1999 Entwicklungsdienstleistungen für den Antriebsstrang, Sicherheits-, Komfort- sowie elektrische und elektronische Systeme auf Basis erprobter Bosch-Großserientechnik und ist Systementwicklungspartner der Automobilindustrie.

Chancen erkennen und sinnvoll nutzen – vernetztes Engineering in der Automobilindustrie

Milliarden Dinge auf der Welt tauschen sich heute schon aus und teilen Informationen, z. B. Autos oder Smartphones. Dinge werden immer mehr zum aktiven Teil des Internets. Wie das gelingt? Jedes „Ding“ auf der Welt kann Daten ins Netz schicken und mit jedem anderen „Ding“ kommunizieren, um vielfältige Aufgaben für seinen Besitzer zu erledigen.

Im Internet der Dinge (Internet of Things, IoT) verschmelzen physische und virtuelle Welt. Das IoT wächst rasant und weltweit. Dies führt zu enormen Veränderungen und bietet gleichzeitig neue Chancen für die Wirtschaft. Heute sind laut Forschungsinstitut Gartner bereits rund sechs Milliarden Dinge auf der Welt vernetzt. Bis 2020 sollen es mehr als 20 Milliarden Dinge sein. Der IoT-Markt wird schon 2020 rund 250 Milliarden US-Dollar erwirtschaften. In der Automobilindustrie erleben wir derzeit diesen Übergang hin zu neuen Formen der Mobilität. Elektrifizierung, Vernetzung, neue Konzepte von Mobilitätsservices sowie die Integration einer digitalen Kultur gewinnen zunehmend an Bedeutung und sind in der Öffentlichkeit viel diskutierte Themen. Die Auswirkungen von IoT sind bereits heute überall sichtbar und für jeden unmittelbar erfahrbar. Das Internet der Dinge macht das Leben der Menschen komfortabler, sicherer und die Wirtschaft effizienter und ressourcenschonender. Ziel ist, Produkte und Services Schritt für Schritt zu vernetzen, auch mit Hilfe von Cloud-Computing. Mit vernetzten Produkten und Lösungen lässt sich das traditionelle Geschäft weiterentwickeln. Zudem lassen sich neue Geschäftsmöglichkeiten erschließen, allen voran Dienstleistungen.

In der Automobilindustrie profitieren wir stark von den zahlreichen Möglichkeiten, die die Digitalisierung und Vernetzung mit sich bringen. Moderne Fahrzeuge sind mit einer Vielzahl an Fahrerassistenzsystemen, die dem Fahrer in Fahr- und Parksituationen helfen oder Aufgaben teilweise komplett übernehmen, ausgestattet. Die innovativen Assistenzsysteme sorgen damit für mehr Komfort und vor allem für mehr Sicherheit für den Fahrer. So ist seit April dieses Jahres für alle Neuwagen das eCall-Notrufsystem verpflichtend. Das System setzt selbstständig nach schweren Unfällen einen Notruf ab – mit den exakten Standortdaten des verunfallten Autos. Die Digitalisierung zieht sich quer durch alle Arten von Dienstleistungen und Produkten der Automobilindustrie. Für die Vielzahl an Tests und Messungen von Emissionen haben wir spezielle Verfahren entwickelt. Mit diesen können wir die Vielzahl von realen Straßentests digital mittels

INTERESSE GEWECKT?
Melden Sie sich bei der **DIGITALE WELT** Redaktion via E-Mail unter blog@digitaleweltmagazin.de oder telefonisch +49 89 2180 9171



Simulationen in eine reproduzierbare Umwelt bringen und die komplexen Antriebssysteme noch spezifischer untersuchen und weiter optimieren – um Emissionen künftig noch stärker zu minimieren. Per Telemetrie werden im Motorsport Daten direkt aus dem Rennwagen zu den Ingenieuren in die Boxengasse übertragen. Das Rennteam ist damit in der Lage während des Rennens bestimmte Funktionen in Echtzeit zu überwachen, zu kalibrieren sowie direkte Auswertungen für eine ausführliche Fehleranalyse durchzuführen. Die Technik funktioniert ähnlich wie bei einem Smartphone, nur viel schneller.

Unser Kerngeschäft liegt in der Entwicklungsdienstleistung für Pkw. Über die Jahre haben wir jedoch unser Portfolio über sämtliche Fahrzeugsegmente ausgebaut. Unser Ziel dabei ist, die Expertise sowie Technologien aus dem Automobilumfeld, gepaart mit IoT-Lösungen, auf andere Fahrzeugsegmente zu übertragen. Wie eng verzahnt alles miteinander ist, lässt sich am Beispiel des vernetzten Güterzuges erläutern. Heutzutage sind im Cargobereich Züge und Waggons intelligent untereinander sowie mit ihrer umgebenden Infrastruktur vernetzt. Mittels eines intelligenten Vernetzungssystems wissen die Wagen daher von selbst, wann sie an ihrem Ziel ankommen, ob die Kühlkette eingehalten wird und sie übermitteln Informationen, mit denen der Termin zur nächsten Instandhaltung bestimmt wird. Via Cloud werden die Daten direkt in ein Onlineportal des Bahnbetreibers übertragen. Aber auch Lösungen aus dem automatisierten Fahren und der Fahrerassistenzsysteme fließen ein. So können künftig Güterwaggons automatisiert im geschlossenen Depot oder Rangierbahnhof ohne Fahrer bewegt werden. Ein Kollisionsswarmsystem unterstützt Zugführer bei den Rangierarbeiten. Erfolgreich im Einsatz ist dieses System auch bei Straßenbahnen. Hier warnt das System den Fahrer beispielsweise auf Fahrten durch belebte Innenstädte frühzeitig vor Autos oder Fußgängern auf den Gleisen. Die dafür eingesetzte hochmoderne Umfeldsensorik wurde aus dem automatisierten Fahren speziell für den Einsatz im Zug weiterentwickelt.

Wie vielfältig der Einsatz unserer Technologien sein kann, zeigt das Beispiel des vernetzten Ackers: Die digitale Technologie erleichtert den Arbeitsalltag von Landwirten und unterstützt dabei, den optimalen Zeitpunkt für die organische Düngung zu finden, exakt zu bewässern sowie den idealen Reifegrad für die Ernte festzulegen. Mit unseren speziellen Sensorsystemen überwachen Landwirte ihre Felder. Das System misst über und unter der Erde Temperatur, Sonneneinstrahlung oder den Wasserstress der Pflanzen. Via Tablet oder Smartphone hat der Landwirt die ständige Kontrolle über die Parameter seiner Pflanzen. Dazu gehört auch die Benachrichtigung darüber, wenn ein Messwert den definierten Alarmwert überschreitet.

Stand heute sind bereits eine Vielzahl unserer Technologien und Produkte miteinander vernetzt. Ein nächster Schritt ist, auch die Entwicklungsprozesse noch enger zu vernetzen. Mit Blick auf die Fahrzeugentwicklung lässt sich dies über offene Entwicklungsplattformen umsetzen. Diese kombinieren alle relevanten Tools, Workflows und Daten zur Entwicklung. Die Tools dienen dabei zur vernetzten Entwicklung, Analyse und Auswertung sowie zum Reporting und zur Kollaboration. Die Entwicklungs- und Testingenieure sind somit direkt mit den Fahrzeugen vernetzt, unabhängig von ihrem Standort. Dieses räumlich entkoppelte Arbeiten bringt weitere Möglichkeiten und Vorteile mit sich. Die Nutzung von Entwicklungsfahrzeugen kann deutlich effizienter erfolgen. Automobilhersteller benötigen keine riesigen Testflotten, die bei verschiedenen Dienstleistern für die Analysen und Tests im Einsatz sind. Über eine offene Onlineplattform sind alle relevanten Tools für die Entwickler nutzbar. Die Teams können somit flexibel und standortunabhängig zur selben Zeit auf das gleiche Fahrzeug zugreifen und verschiedene Messungen und Tests durchführen. Ein weiterer Vorteil solcher Plattformen ist das gemeinsame Nutzen der Daten. Analysen und Auswertungen können einfach und bequem über die Plattform von allen Entwicklern eingesehen und genutzt werden. Ein simultanes und flexibles Engineering wird durch die Vernetzung möglich.

Diese Form des Arbeitens lässt sich auch auf andere Industriebereiche übertragen. Entwicklerteams können somit von Standorten weltweit über eine gemeinsame Onlineplattform an einem Projekt arbeiten, unabhängig und entkoppelt von Maschine oder Fahrzeug. Für die Fahrzeugindustrie heißt das, dass Automobilhersteller, Zulieferer und Entwicklungsdienstleister künftig das Thema Onlineplattformen vorantreiben sollten, um eine gemeinsame Entwicklungsarbeit weiter zu optimieren.

Foto: Wolfram Scheible

Projektplanung 4.0 mit Skills und künstlicher Intelligenz

Dass eine auf realistischen Angaben beruhende Projekt- und Ressourcenplanung kein Hexenwerk ist, beweist die Münchner Softwareschmiede Can Do.

Mit der gleichnamigen Software setzt das IT-Unternehmen dem vielzitierten War for Talents eine Lösung zur skillbasierten Kapazitätsplanung entgegen. Damit gelingt die exakte Zuweisung der geeigneten Mitarbeiter in fach- und standortübergreifenden Projekten mühelos. Zunächst müssen die vorhandenen Fähigkeiten allerdings an zentraler Stelle in einer sogenannten Skill-Bibliothek erfasst werden. Diese dient als Datenpool, um geeignete Mitarbeiter zu finden, und soll auf Knopfdruck Aussagen

zum Skill-Bestand, Skill-Bedarf und möglichen Qualifizierungslücken liefern. So kann das Management vorteilhaft planen und die in Zukunft benötigten Fähigkeiten durch geeignete Weiterbildungsmaßnahmen frühzeitig aufbauen. Hiervon profitieren auch die Mitarbeiter, indem sie eine Art „Glaskugel“ für ihre Karriereplanung erhalten und sehen, welche ihrer Skills im Unternehmen langfristig gefragt sind. Sie können über Fortbildungen diese Fähigkeiten erwerben und ihren Karriereweg strategisch planen.

Den Umgang mit der fortschreitenden Komplexität im Planungsalltag verein-

facht Can Do mit Handlungsempfehlungen. Mittels künstlicher Intelligenz raten diese zum Ignorieren oder sofortigen Eingreifen im Falle eines Risikos. So behalten Anwender auch bei vielschichtigen Aufgabenstellungen den Überblick und treffen schnelle und gute Entscheidungen. Von Entmündigung kann dabei keine Rede sein. Lediglich analysiert die Software die vielfältigen planerischen Abhängigkeiten schneller und umfassender, als es ein Mensch je könnte. Nächster Schritt: Can Do goes Cloud.

Florentina Hofbauer

Foto: CanDo



Das Gesicht durch Lichtprojektionen zu schminken ist eine Technik, die bei berühmten Bühnenkünstlern immer beliebter wird.

Projection Mapping im Gesicht: Face-Hacking

Face-Hacking eröffnet sprichwörtlich eine neue Dimension von Augmented Reality. Sie erzielt einen Grad der Immersion, welche sogar den einer AR-Brille übersteigt.

Projection Mapping – auch Projektionsmapping genannt – ist eine Technologie, in der Licht auf eine unebene Oberfläche projiziert wird: So können beispielsweise spektakuläre Werbefilme eindrucksvoll auf Gebäude projiziert werden. Liebhaber von Lichtspielen ist diese Technologie schon länger ein Begriff. Face-Hacking – auch „special augmented reality“ oder „video mapping“ genannt – ist nun eine spezielle Form des Projection Mappings. Erst seit Kurzem hat sich diese Digitale

Technologie so weit entwickelt, dass sie eindrucksvoll einsetzbar ist.

Kunst im Gesicht

Beim Face-Hacking handelt es sich um Echtzeit-Projektionen welche auf dreidimensionale Objekte geworfen werden, anders gesagt: Durch einen Beamer und somit nur mit Licht, kann man eine Person schminken. Dafür werden zuerst kleine Sensoren auf dem Gesicht angebracht. So wird dieses gewissermaßen in eine dreidimensionale Leinwand verwandelt. Künftig könnten

Bühnenkünstler auf diese Weise in andere Rollen schlüpfen, ganz ohne dafür extra ihre Maske zu ändern. Auch Modeschauen könnten völlig anders ablaufen als bisher gekannt. Die neue Technik eröffnete unendliche neue kreative Räume. So stellt sich hier einmal mehr die Frage, ob Mensch und Maschine bald gemeinsam künstlerisch tätig sein werden. Denn es gibt bereits Computerprogramme die Bilder malen, Bots die komponieren oder Apps die Gedichte schreiben.

Florentina Hofbauer

Foto: Pixabay

DIGITALISIERUNG in Zahlen



25 % aller sozialversicherungspflichtig Beschäftigten haben ein hohes Risiko, dass ihre Tätigkeit in absehbarer Zeit durch Automatisierung ersetzt wird.



3.100 Google-Mitarbeiter haben sich in einem offenen Brief gegen die militärische Nutzung von künstlicher Intelligenz durch Google ausgesprochen.



Der Umsatz des deutschen Videospielmarkts lag im vergangenen Jahr erstmals bei über **3 Mrd. Euro.**



Der kanadische Hersteller von Quantencomputern, D-WAVE, sammelte bislang **220 Millionen US-Dollar** an Investitionen.



Ab November 2020 müssen Auftragnehmer von Behörden ihre Rechnungen über 1000 Euro oder mehr elektronisch ausstellen.

78 % aller Unternehmen in Deutschland, Österreich und der Schweiz gehen davon aus, dass das Internet of Things (IoT) innerhalb der kommenden drei Jahre wichtig bis sehr wichtig wird.

BMW will in

3 Jahren

ein autonomes Auto in Serie bringen.



5 Milliarden US-Dollar investiert Microsoft in den kommenden vier Jahren in das Internet der Dinge.



Zwischen den Jahren 2011 und 2016 haben Technologieinvestitionen die Anzahl der Beschäftigten noch um

1 % erhöht.



Laut einer OECD-Studie weisen **45 %** der Deutschen eine niedrige Kompetenz in technologiebasiertem Problemlösen auf (OECD-Durchschnitt 45 %).

Eine Studie einer US-Behörde sagte für den Quantum-Computing-Markt bis 2024 ein jährliches Wachstum von über

24 % voraus.



44 % der Unternehmen geben Sicherheitsbedenken als größte technische Herausforderung für IoT-Projekte an.





Very digital Person: SAMI HADDADIN

Sami Haddadin gilt als einer der bedeutendsten Roboterforscher der Welt, dessen Pionierarbeit die Robotik revolutioniert hat.

Der Robotikforscher Sami Haddadin wurde Ende vergangenen Jahres zusammen mit seinem Team vom Bundespräsidenten Frank-Walter Steinmeier für seine revolutionären Entwicklungen im Bereich der Robotik mit dem Deutschen Zukunftspreis gekürt. Im Interview mit dem DIGITALE WELT Magazin spricht der Universitätsprofessor über seine Arbeitsweise, seine Zukunftsvision, die gesellschaftliche Verantwortung in Bezug auf die neuen Technologien sowie den großen Unterschied zwischen seinen Assistenzsystemen und Robotern aus Hollywood-Filmen.

Haben Roboter schon immer eine Faszination auf Sie ausgeübt? War Ihnen immer klar, dass Sie sich früher oder später mit diesem Thema beschäftigen würden?

Nein, nicht wirklich, nicht als Kind. Mich haben die Naturwissenschaften interessiert, also Biologie und Physik. Ich dachte immer, dass es interessant wäre, das intelligente Leben zu erforschen, also zum Beispiel das, was den Menschen ja so interessant macht. Auf der Hannover Messe habe ich Ende der neunziger Jahre eine filigrane Roboterhand gesehen, die dort ausgestellt war. Und nach und nach habe ich gemerkt, dass es doch die Roboter waren, die mich interessieren, und hier gerade ihr Bezug zum Menschen. Denn die Fragen nach dem Menschen trieben mich weiter um: Wieso sind wir so komplex aufgebaut? Was sind zum Beispiel die Prinzipien der Hand? Wieso ist der Mensch so kreativ und innovativ? Die Ingenieurwissenschaften und hier insbesondere die Robotik können als Werkzeuge des Erkenntnisgewinns doch viele Antworten darauf geben, was den Menschen so einzigartig macht.

In einem Fernsehinterview haben Sie Ihre Innovation als eine „Enabler-Technologie“ bezeichnet, die uns ein neues

Zeitalter eröffnen wird. Wird dieses „Zeitalter der Roboter“ Ihrer Meinung nach noch schneller voranschreiten, als das Zeitalter der Digitalisierung es in den letzten 20 Jahren getan hat?

Mit Enabler-Technologie meine ich Meilensteine in der Entwicklungsgeschichte der Menschen und die sind gekoppelt mit gewissen Werkzeugen. Digitalisierung ist eine Vorstufe des Zeitalters der Maschinen und Roboter. Die ursprüngliche Enabler-Technologie ist sicherlich das Internet. Deshalb wird das Zeitalter der Roboter-Technologien vielleicht nicht unbedingt schneller, aber doch intensiver voranschreiten. Ich glaube, dass die Digitalisierung auch deswegen schnell voranschreitet, weil es sich in vielen Fällen um rein virtuelle Güter dreht. Die intelligente Maschine ist wieder der Kreisschluss, um das Virtuelle in die physische Welt zu bringen. Auch einige der Trends der Digitalisierung werden die Art und Weise wie Robotik begriffen wird stark beeinflussen und bestimmen. Das sieht man schon jetzt in den Roboter-Verkaufszahlen, die sehr stark ansteigen. Man merkt hier auf jeden Fall eine starke Aufbruchsstimmung. Ich denke, dass in der Robotik das Potenzial liegt, eine große Indus-

trie zu schaffen. Vergleicht man Robotik heute mit Elektronik und Automobilen, so sehen wir noch eine vergleichsweise kleine Industrie. Um ein Beispiel zu nennen: Es werden etwa gleich viele Industrieroboter verkauft, wie Autos von Porsche. Und das ist ja nur eine, und zwar eine Luxusmarke unter vielen. Die Industrierobotik ist Stand heute also noch ein Luxusgut, auch wenn jetzt ein Demokratisierungsprozess beginnt. Irgendwann werden Roboter in jedem Haushalt existieren. Es gibt erste Beispiele dafür, etwa die mit der Drohnen-Technologie, die sich schon heute viele Menschen leisten können, oder eben die Rasenmäher- oder Staubsauger-Roboter. Es gibt hier zunehmend stark wachsende Bereiche.

Welche Aufgaben können Roboter langfristig übernehmen und wann werden die Ergebnisse Ihrer Forschung in der Allgemeinheit ankommen?

Die eigentliche Frage ist: Was ist der nächste Schritt? Der nächste Schritt ist, dass Roboter in der gesamten industriellen Fertigung ankommen werden. Dass also kleine und mittelständische Unternehmen auch Zugang zu solchen neuartigen Robotern bekommen. Gerade bei den deutschen Hidden Champions könnten viele Roboterassistenten eingesetzt werden. Ich beobachte, dass unsere Forschung von vor nunmehr zehn Jahren immer weiter in die reale Welt eindringt, sehen Sie sich allein die Mensch-Roboter-Kollaboration an. So gibt es eine wachsende Zahl kleiner und mittelständischer Unternehmen, die heute Roboter schon einsetzt. Das ist ein Prozess, der jetzt in der Arbeitswelt Einzug hält. Wichtig ist, dass die Menschen auch im Umgang mit der Technologie geschult werden. In den nächsten fünf bis zehn Jahren wird es große Schritte im Health-Care-Bereich geben, etwa in der Logistik von Krankenhäusern. Ein weiteres gutes Beispiel in diesem Sektor ist die Rehabilitation von Schlaganfall-Patienten. Da es nur eine beschränkte Menge an Fachpersonal mit der entsprechenden Ausbildung für diese Patienten gibt, können Roboter-Assistenzsysteme dabei helfen, den Einsatz der Experten zu flexibilisieren und sie effizienter zu nutzen. Der Roboter operiert also als eine Art Werkzeug. Auch Chirurgie und Prothetik sind große Anwendungsgebiete der Robotik. Auch könnten Roboter-Assistenzsysteme mittel- und langfristig dabei helfen, dass Senioren länger selbstbestimmt zu Hause wohnen bleiben können, indem sie ihnen den Alltag erleichtern. Tragischerweise sind Menschen oft unverschuldet gezwungen, im Seniorenheim zu leben, obwohl sie noch aktiv am Leben teilhaben könnten und nur eine Hilfe im Alltag bräuchten. Also Systeme, die beispielsweise dabei helfen, den Geschirrspüler ein- und auszuräumen, Dinge vom Boden zu heben oder beim Aufstehen zu helfen. Die ersten Service-Robotik-Anwendungen, gerade im Haushalt, gibt es ja nun auch schon. Insgesamt wird der Trend dahin gehen, dass zahlreiche Technologien zuerst in der Industrie und dann in den Haushalten Einzug finden werden.

„Ich dachte immer, dass es interessant wäre, das intelligente Leben zu erforschen, also das, was auch den Menschen so geheimnisvoll und interessant macht.“

Wer haftet dafür, wenn ein medizinischer Roboter einen Aussetzer hat?

Produkthaftungsgesetze gelten bei Roboter-Assistenzsystemen genau wie bei anderen Systemen. Insgesamt lässt sich aber in Bezug auf die Produkte sagen, dass der Inverkehrbringer haftet. Natürlich ist es unabdingbar, dass Juristen und Technolo-

gen sich beim Thema Haftung eng vernetzen. Deshalb haben wir beispielsweise den Verein RAILS gegründet. Das steht für „Robotics & AI Law Society e. V.“. Dieser Verein hat eine fachübergreifende Ausrichtung, es wird hier also interdisziplinär zusammengearbeitet. Wir wollen intelligente Systeme von Anfang an verantwortungsvoll entwickeln und von Anbeginn sinnvolle, maßvolle und technisch umsetzbare Rechtsrahmen diskutieren. Bei diesen Dingen müssen die Juristen am Ende ja auch den Expertenblick kommunizieren. Das sind wichtige Thematiken, die zurzeit überall hochkochen, jedoch mit dem richtigen Verantwortungsbewusstsein angegangen werden müssen. Positiv ist, dass die EU in der diesbezüglichen Diskussion von Gesetzgebung schon ziemlich weit ist. Hier gilt: bloß kein vorausseilender Gehorsam und keine Schnellschüsse, die unserem Standort im Nachhinein wieder schaden.

In Zeiten von Hacker-Angriffen und Viren-Befällen: Wie gefährlich ist es, auf Medizinroboter oder Roboter als Lebenshilfen zu vertrauen?

Sicherheit ist einer der wichtigsten Aspekte in der Roboter-Entwicklung. Man geht als Robotik-Experte natürlich mit IT- und Security-Experten an diese Herausforderung heran. Am Ende des Tages muss beim Systemdesign sehr viel Safety und Security mitgedacht werden. Wenn man diese Aspekte frühzeitig im Design berücksichtigt, dann ist es natürlich einfacher. Es gibt viele Barrieren die eingebaut werden können, damit die Roboter-Assistenzsysteme schwierig zu hacken sind. „Unhackbar“ ist natürlich nichts, da sollte man sehr realistisch bleiben. Das interessante ist aus wissenschaftlicher Sicht jedoch, dass man in Robotern die Physik sehr gut nutzen kann, um die Systeme sicherer zu machen. Der Roboter kann nämlich

prüfen, ob das Gesehene noch physikalisch sinnvoll ist und so gewissermaßen seine eigene Security überprüfen.

Man muss keine Programmierkenntnisse haben, um Ihre Roboter binnen einer halben Stunde programmieren zu können. Haben Sie hierfür eine gänzlich neue intuitive Programmiersprache entwickelt?

Ja, wir haben eine neue Roboterprogrammiersprache und ein neues Technologiekonzept zu ihrem Einsatz entwickelt.

Geworben wird damit, dass Garmi bald die Spülmaschine ausräumt und die Mikrowelle bestückt. Fördert das nicht auch, dass Menschen sich noch weniger bewegen und dadurch früher krank werden?

Geworben wird gar nicht, denn Garmi wird noch über Jahre entwickelt und weiterentwickelt. Mit dem Deutschen Zukunftspreis werden ja wissenschaftlich-technische Entwicklungen, die einen großen Einfluss auf unsere zukünftige Gesellschaft haben werden, prämiert. Also ist die Frage wichtig, wie man auch den Senioren verständlich machen kann, was wir hier tun und ihnen bewusst macht, welche konkreten Vorteile sie haben. Das kann natürlich nicht nur erklärt werden, sondern das muss man erfahrbar machen. Finnland ist hierbei immer in gewisser Weise mein Vorbild. In Finnland haben Senioren schon Mitte/Ende der Neunziger selbstverständlich E-Mail- und Handykurse erhalten und somit schon früh Fähigkeiten im Umgang mit dieser neuen Technologie besessen. Es ist ja auch eine gesellschaftliche

Aufgabe unsere Senioren und unsere Jugend an neue Technik heranzuführen. Es ist definitiv eine Frage, die wir proaktiv beantworten müssen. Heutzutage spielt die menschenzentrierte Robotik eine große Rolle. Es ist dann doch erstaunlich, wie hoch die positive Resonanz, wenn man den Vorteil dieser neuen Assistenten herausstellt, doch ist. Aus unterschiedlichsten Umfragen geht hervor, dass Senioren sehr wohl einen Roboter einsetzen würden, um die Möglichkeit zu haben, weiterhin selbstbestimmt zu Hause leben zu können. Der Punkt ist ja, dass der Roboter, von dem wir sprechen, ein Assistenzsystem ist. Auch in der Chirurgierobotik operiert kein Roboter, sondern natürlich der Chirurg. Der Roboter hält zwar das Skalpell, aber der Arzt steuert den Roboter direkt als Werkzeug. Haushaltsgeräte sind ja gewissermaßen auch Assistenztechnologien und eine Möglichkeit, mehr Zeit für uns zu haben. Sie erleichtern den Alltag und erlauben mehr Zeit für menschliche Interaktion und Zuwendung zu haben. Menschen glauben oft, hier spielt natürlich die Science Fiction eine große Rolle, dass Roboter morgen unseren Alltag übernehmen könnten, aber so ist es bei realistischer Betrachtungsweise definitiv nicht. Wir entwickeln ja keinen Ersatz für Menschen, sondern ganz im Gegenteil Assistenzsysteme für den Menschen. Das hat der Mensch schon immer gemacht und wir nennen das Werkzeug und ihre Demokratisierung ist ein wichtiger Baustein.

Die Entwicklung lässt vor allem Arbeiten von klassischen Geringverdienern überflüssig werden. Sie jedoch sprechen von einem Demokratisierungsprozess in Bezug auf Ihre neue Technologie: Wie begegnen Sie entsprechenden Ängsten?

Unsere Industrie und die Arbeitsplätze werden nicht wegrationalisiert, sondern es werden neue Dinge entstehen, die bis gestern gar nicht möglich gewesen wären. So bin ich beispielsweise ganz anders aufgewachsen als meine Kinder heute, das ist der Lauf der Dinge, und technische Innovation, Wissenschaft und Erkenntnisgewinn sind wichtige Eckpfeiler unserer Gesellschaft und Identität. Wir müssen diese Ängste natürlich ernst nehmen und mit ihnen rational umgehen. Typischerweise haben die Menschen ja beispielsweise Roboter aus dem Film „I, Robot“ im Kopf. Daher müssen wir vor allem darauf achten, dass die Menschen informiert sind und richtig ausgebildet werden. Gerade auf die Fragen und Herausforderungen der Robotik sind wir doch immer besser vorbereitet: mit dem Pilotprojekt Roboter-Fabrik, einer Lernfabrik und Begegnungsstätte für Robotik, die die nächsten Jahre flächendeckend eingesetzt werden soll. Die Ängste müssen den Menschen auch deshalb genommen werden, weil wir in einem Hochtechnologieland wie Deutschland darauf achten sollten, dass wir eine technologische und wissenschaftliche Vorreiterrolle einnehmen und ausfüllen. In Bezug auf Internet-Technologien sind wir vor allem Konsumenten und Treiber der Innovation. Dabei sollten Dinge, die auch hier mitentstanden sind, in Deutschland in der Wertungskette bleiben. Das ist auch eine Verantwortung gegenüber unserer Zukunft sowie der nächsten Generationen. Wir sollten doch ein Interesse daran haben, dass die großartigen Technologien, die hier kontinuierlich entstehen, hier auch umgesetzt werden, und wir sie dann natürlich in die ganze Welt verkaufen: Zentrale Teile der Wertschöpfungskette, neben der Forschung und Technolo-

gie also die Produktion und die verbundenen Arbeitsplätze, sollen hier entstehen und bleiben. Speziell weil wir nicht nur sehr gute Informatiker, sondern insbesondere auch hervorragende Ingenieure in Deutschland haben. Es geht ja nicht nur um den derzeitigen Trend der künstlichen Intelligenz, sondern um die sogenannte maschinelle Intelligenz. Mechatronik, Robotik, maschinelles Lernen und künstliche Intelligenz: All das gipfelt ja in maschineller Intelligenz. In dieses Thema brauchen wir mehr Investitionen, und wir sollten eine Führungsrolle einnehmen.

Ihr Roboter besteht aus ultraleichten Komponenten. Welche Materialien haben Sie benutzt und mit welchen Materialien haben Sie experimentiert? Wieso ist Ihre neue Roboter-Generation viel kostengünstiger, als die bisherigen Modelle?

Weil es sich um einen holistischen systemischen Design-Prozess handelt, der keine unnötigen Unterscheidungen zwischen Soft- und Hardware macht. Im Grunde haben wir eine Art Roboter-Compiler entwickelt, der ausrechnet, welche technologischen Komponenten die besten sind, um entsprechende Ziele im Sinne der gewünschten Roboterfähigkeiten zu erreichen. Das ist eine noch nicht besonders verbreitete Denkweise. Viele der Schritte im Designprozess sind auch sehr menschenzentrisch. Der Roboter ist ein holistisches, mit dem Menschen interagierendes Gesamtsystem. Gesagtes gilt natürlich auch in Bezug auf die Einbeziehung der Kosten. Dieses System zieht sich durch bis zum Produktionsprozess, sodass die Roboter obzwar großer Stückzahlen wirtschaftlich in Deutschland gefertigt werden. Grundsätzlich möchte man immer das Optimum herausholen, und zwar primär in der Performance, nicht in den

Kosten. Nur weil der Roboter eine gewisse Fähigkeit erlernt, soll er nicht auf eine andere verzichten müssen. Mittlerweile können die Roboter beispielsweise schon motorische Fähigkeiten erlernen, in etwa so wie bei einem drei- bis vierjährigen Kind.

Ihre Vorlesungen halten Sie auf Englisch, Ihre Dissertation haben Sie ebenfalls in englischer Sprache verfasst. Gibt es überhaupt genügend deutsche Ausdrücke und Wörter, die Ihre revolutionäre Arbeit hinreichend beschreiben würden?

Ganz im Gegenteil. Meine Vorlesungen halte ich nicht immer auf Englisch. Eigentlich finde ich es sogar sehr interessant Wörter zu finden, die es im Deutschen so noch gar nicht gibt. Beispielsweise habe ich kürzlich den sogenannten „Fernkörper“ eingeführt. Heute ist man ja im Grunde bei der körperlosen künstlichen Intelligenz und es geht hin zu einer verkörperten Intelligenz. Dies hat sehr viel mit dem Konzept der Verkörperung „embodiment“ zu tun und dieses in der Zukunft aus der Ferne zu steuern. Man könnte auch von einem Avatar sprechen. Lange Zeit hat mir das Wort nicht gefallen, weil dann alle wieder aufgrund von Science-Fiction-Filmen an blaue Außerirdische denken. Also war der Schritt von der Verkörperung zur „Fernkörperung“ nicht mehr weit: Mittels neurotaktile Interfaces, die breitbandig und mit minimaler Latenz mit lernfähigen Robotern verbunden sind, können Sie sich dann beispielsweise in Gefahrengeländen wie Fukushima aufhalten und agieren als wären Sie vor Ort, ohne sich der gefährlichen Strahlung auszusetzen. Die Anwendungen sind ja fast grenzenlos.

Florentina Hofbauer

Foto: Leibniz Universität Hannover



DIST DAS SCHON BURNOUT?

Eine weibliche Führungskraft, 42 Jahre, Teamleiterin im Controlling, suchte Unterstützung für folgende Problemstellung: Sie war vor sechs Monaten zur Leiterin des Teams befördert worden, in dem sie selbst als Teammitglied viele Jahre aktiv war. Mit den meisten Mitgliedern des Teams hat sie über die Jahre ein nahezu freundschaftliches Verhältnis aufgebaut. Es gibt jedoch einen Kollegen, der sich seit der Beförderung merkwürdig verhält: Er hat sich stark zurückgezogen, achtet streng auf die Einhaltung formaler Wege und beäugt sie in Besprechungen kritisch. Sie hat den Eindruck, dass er auf Fehler ihrerseits wartet, um sie dann „in die Pfanne zu hauen“.

Das verunsichert sie sehr, zumal sie auch eine gewisse Reserviertheit der anderen Teammitglieder spürt. Darüber hinaus wird sie von ihrer Chefin unter Druck gesetzt, die anstehenden Umstrukturierungen von Aufgaben und Prozessen auf den Weg zu bringen. Die Situation trägt seit einigen Wochen zu schlaflosen Nächten bei.

Die Balance – beruflich, privat, persönlich – ist in Schieflage

Zusätzlich zu ihren beruflichen Problemen hat sie mit ihrer pubertierenden Tochter immer wieder Auseinandersetzungen, die sie viel Kraft und Energie kosten. Sie fühlt sich zunehmend erschöpft, kann sich auch am Wochenende nicht mehr wie früher regenerieren.

So ist sie also zur Hausärztin gegangen, die ihr einen Burnout bescheinigt. Mit einer Krankschreibung für 14 Tage und einem Rezept für ein Psychopharmaka findet sie sich zu Hause wieder und ist völlig irritiert.

Beim Lesen des Beipackzettels bekommt sie es mit der Angst vor den Nebenwirkungen zu tun. Sie beschließt, das Präparat nicht einzunehmen und doch lieber die vom Unternehmen angebotene anonyme Coaching-Hotline zu kontaktieren – ein Anruf, vor dem sie sich bis jetzt gescheut hatte.

Der Anruf bei der Coaching-Hotline lohnt sich

In der ersten „Face-to-Face“-Coaching-Einheit werden die beruflichen, privaten und persönlichen Problemstellungen

konkret sortiert sowie für jedes Feld ein persönliches Ziel formuliert.

In den folgenden Coaching-Einheiten werden Maßnahmen entwickelt, die dann in Folge umgesetzt werden. Zur Klärung der beruflichen Konflikte sucht die Klientin im ersten Schritt das offene Gespräch mit ihrer Chefin. Im Ergebnis wurde ein Führungswechsel-Workshop vereinbart, der zu einer Klärung von Erwartungen und Rollen des Teams und der Teamleiterin führt.

Der „kritische“ Kollege hatte sich tatsächlich Hoffnung auf den Job als Teamleiter gemacht. In einem Gespräch zu dritt zwischen ihm, Teamleiterin und Chefin findet eine Konfliktklärung statt, die eine erste Erleichterung bringt.

Auf persönlicher Ebene „verordnet“ sich die Klientin selbst ein Programm zur aktiven Regeneration ihrer Energien. Mit kleinen Zeitfenstern pro Woche vereinbart sie Termine mit sich selbst, in denen sie zu Hause wieder ihre Yoga-Übungen macht, die ihr früher schon immer besonders gutgetan haben. Auf dem Weg zur Arbeit hört sie über Kopfhörer bewusst ihre Lieblingsmusik, um beschwingt anzukommen. Vor dem Heimweg reflektiert sie gedanklich die Aufgaben, die sie am Tag erledigt hat. Am Wochenende verabredet sich sie mit Freunden zu gemeinsamen Aktivitäten, für die sie in den vergangenen sechs Monaten zu müde war. Im Kontakt zu ihrer Tochter erinnerte sie sich daran, dass es durchaus auch viele spannungsfreie und schöne Momente gab, und die unangenehmen buchte sie auf das Konto „Pubertät bedeutet Großbaustelle im Gehirn“ und versuchte, sie nicht zu wichtig zu nehmen.

Der gesamte Coaching-Prozess umfasste acht Einheiten und brachte für die Führungskraft, ihr Team und ihr Privatleben einen vollen Erfolg.

Niederschwellige professionelle Coaching-Angebote sind wichtiger denn je, damit möglichst frühzeitig „Schieflagen der persönlichen Balance“ aufgefangen werden. Es lohnt sich!

Dr. Petra Bernatzedler,
Diplom-Psychologin, Geschäftsführung
upgrade human resources GmbH

Messe München – der gekonnte Mix aus digital und real

Auf einer Messe zeigt man heute mehr, als nur seine Produkte. 360-Grad-Kameras oder VR-Brillen bieten Messebesuchern ein völlig neues Erlebnis. Denn die Messe München entwickelt sich ständig weiter und vergisst dabei nicht seine Mitarbeiter: So erreicht der digitale Wandel alle Unternehmensbereiche.

Das Messengeschäft hat sich gewandelt: Längst geht es um mehr als das Verkaufen von Ausstellungsflächen. Der Vorsitzende der Geschäftsführung der Messe München, **Klaus Dittrich**, spricht im Interview mit dem DIGITALE WELT Magazin über Unternehmensführung, neue Geschäftsmodelle und die Relevanz von Kreativität im digitalen Zeitalter.

Wie ist Ihre persönliche Haltung zur Digitalisierung?

Ich sehe in der Digitalisierung eine große Chance und eine Bereicherung für unser Leben. Wir befinden uns in der größten Transformationsphase der Geschichte, eine Herausforderung für die Menschheit, für

die es keine vergleichbare Erfahrung gibt, die uns ein hohes Maß an Neuorientierung abverlangt. Die Digitalisierung wird alle Lebensbereiche grundlegend verändern. Im Businessumfeld mache ich die Digitalisierung zur Chefsache: Die digitale Transformation des Unternehmens ist Teil unserer Unternehmensstrategie und damit TOP 1 meiner Agenda.

Sie sehen Digitalisierung also als Bereicherung. Wieso? Viele Leute fürchten sich davor.

Für uns als Messe ist es insofern eine Bereicherung, weil wir dem Kunden über die Quadratmeter Ausstellungsfläche hinaus einen zusätzlichen Nutzen anbieten können – und zwar unabhängig von der Messelaufzeit ganzjährig und 24 Stunden am Tag. Wir leben in einer Zeit, wo sich

wahnsinnig viel verändert. Nun weiß ich natürlich, dass viele Leute Angst vor Veränderung haben. Dabei sollten wir viel besser eine Anleihe bei Kindern nehmen und wie die sich freuen, wenn sie etwas Neues gelernt haben, etwa zum ersten Mal krabbeln oder sprechen können. Aber irgendwann geht offenbar vielen Menschen die Freude am Neuen verloren. Ich finde, man muss diese Freude wiederbeleben und versuchen, den Leuten die Angst vor dem Neuen zu nehmen.

Worin sehen Sie die größten Gefahren, worin die größten Chancen sowie Herausforderungen?

Die Chancen sehe ich klar in der Öffnung etablierter Strukturen für Neues. Wir können neue Produkte entwickeln: So haben wir für die Messe München eine Innovation



Mit der VR-Brille wird auf einem Ergometer ein echtes Fahrgefühl simuliert.

Die Messe München, Blick auf den Haupteingang.



konkreten Interessen als Messe München abgestimmt war. Wir konnten also die relevanten Themen besprechen, etwa was wir mit unseren Besucherdaten machen können. Wir waren auch bei Google, um deren Recruiting-Prozesse kennen zu lernen und zu lernen, nach welchen Kriterien Mitarbeiter ausgewählt werden. Mein Schlüsselerlebnis war jedoch der Besuch bei LinkedIn. Dort bekam jeder Teilnehmer eine Weltkarte mit seinen weltweiten Vernetzungen. Nur für mich gab es keine, weil ich zu diesem Zeitpunkt noch nicht bei LinkedIn registriert war. Das war ursprünglich auch eine bewusste Entscheidung von mir. Doch seit ich dort war, habe ich die revidiert und bin seit Ende vorigen Jahres auf LinkedIn aktiv. Ich habe gemerkt, dass das ein wunderbares Kommunikationstool ist: Es geht in die Mitarbeiterschaft hinein, aber auch nach draußen, man kann interessante Informationen generieren und sich selbst sehr gut mit Leuten vernetzen. Man muss es jedoch selber aktiv machen. Ich bin überrascht, wie

gut und gerne ich das mache. Mit LinkedIn planen wir jetzt auch eine Kooperation.

Finden Sie für eigene LinkedIn-Aktivitäten auch Zeit?

Das ist eine Frage der Prioritäten. Einerseits muss man

sich die Zeit dafür nehmen, andererseits muss man aber auch die Zeit limitieren, die man dafür einsetzt. Man muss einfach bewusst damit umgehen, aber es ist gut investierte Zeit.

Zurück zu den Prozessen bei Google: Was davon möchten Sie umsetzen?

Was wir bereits implementiert haben, ist

Journey entwickelt oder ein Makeathon. Als entscheidende Herausforderung, vor die uns die Digitalisierung stellt, sehe ich jedoch die Veränderung der Unternehmenskultur. Sie verlangt Mut zur Veränderung. Entscheidend ist nach meiner Erfahrung dabei, dass alle bis hinauf zum Topmanagement die Möglichkeiten der Digitalisierung, z. B. im Bereich Social Media, selbst auszuprobieren und nicht nur darüber reden.

Gibt es in Ihrem Unternehmen konkrete Maßnahmen, um alle Mitarbeiter ins Boot zu holen?

Wir haben beispielsweise ein Programm namens „Digital Spa“ gestartet. Einmal im Monat gibt es die Möglichkeit für Mitarbeiter, sich von unseren Experten im neuen Geschäftsbereich Digital über digitale Themen informieren zu lassen. Hier wird

beispielsweise das Geschäftsmodell von Facebook erklärt oder die Blockchain-Technologie. Hierbei kann sich jeder Mitarbeiter anmelden, unabhängig von der Abteilung und der Position. Wir haben bislang mehr als 500 Teilnehmer in diesem Programm!

Sie haben im Jahr 2016 eine Reise ins Silicon Valley unternommen. Um was zu tun?

Fünf Führungskräfte der Messe München hatten sich für eine Woche ins Silicon Valley begeben. Es war nicht der übliche „Silicon-Valley-Tourismus“, der mittlerweile schon fast zum guten Ton gehört. Im Gegenteil: Wir haben uns ein Programm zusammenstellen lassen, das auf unsere

„Der Kulturwandel wird von vielen Unternehmen als die größte Hürde für den digitalen Wandel gesehen.“



Die Messe München hat eine der größten Photovoltaik-Dachanlagen der Welt.



Blick in das Atrium zwischen den A- und den B-Hallen während einer Messe: In den 18 Hallen und auf dem Gelände der Messe München ist überall WLAN.

Klaus Dittrich

Klaus Dittrich ist seit Januar 2010 Vorsitzender der Geschäftsführung der Messe München mit rund 1.200 Mitarbeitern weltweit. Darüber hinaus



verantwortet er die Messen BAUMA, ISPO MUNICH, ISPO BEIJING, ISPO SHANGHAI, INHORGENTA MUNICH und EXPO REAL. Der studierte Germanist und Politikwissenschaftler (M. A.) ist Mitglied im Vorstand des Ausstellungs- und Messeausschusses der Deutschen Wirtschaft (AUMA) und Vorsitzender der FKM – Gesellschaft zur Freiwilligen Kontrolle von Messe- und Ausstellungszahlen. Er gehört dem Board of Directors des Weltverbands der Messwirtschaft (UFI) an, ist Mitglied im Präsidium des Wirtschaftsbeirats Bayern, Vorstandsmitglied der Italienischen Handelskammer München–Stuttgart, Vizepräsident des Export-Clubs Bayern sowie des Senats der Wirtschaft und Mitglied der Vollversammlung der Industrie- und Handelskammer für München und Oberbayern. Im Januar 2016 hat ihn die Stadtregierung von Shanghai offiziell zum „Berater für das Messe- und Kongresswesen in Shanghai“ benannt.

Er ist verheiratet und hat zwei erwachsene Kinder. Seine Hobbys sind Bergsteigen, Skifahren, Motorradfahren, Langstreckenlauf und Literatur.

das „Reverse-Mentoring-Programm“. Dabei bekommen alle Geschäftsführer und Bereichsleiter einen Digital-Native-Kollegen als Coach an die Seite gestellt. Das ist ein junger Mitarbeiter im Unternehmen, der mit Social Media vertraut ist. In regelmäßigen Abständen trifft man sich, um von den Digital Natives zu lernen. Es sendet ein starkes Signal ins Unternehmen, wenn auch Mitglieder der Geschäftsführung sich weiterentwickeln und etwas von den Jungen dazulernen. Umgekehrt können auch die Jungen von den Älteren etwas mitnehmen. Dieses Programm hat ungeheuren Zuspruch gefunden.

Ist Recruiting heute schwieriger als früher?
Unsere Personalabteilung hat mir gerade

mitgeteilt, dass wir heuer doppelt so viele Auszubildende einstellen wie im vorigen Jahr – und zwar, weil wir so viele gute Bewerbungen bekommen haben. Das liegt daran, dass wir seit einiger Zeit gezielt Social-Media-Marketing zum Zwecke des Employer Brandings betreiben.

Finden im Silicon Valley direkt auch Messen statt?

Dort gibt es riesige Veranstaltungen: Einerseits Firmenevents, andererseits auch Messen zum Thema Digitalisierung wie beispielsweise die Dreamforce von Salesforce mit über 160.000 Teilnehmern oder die RSA Conference zum Thema Cyber Security. Auch wir planen übrigens eine

„Man sollte darauf achten, alle dazu zu motivieren, sich dieser neuen Welt zu öffnen.“

neue Veranstaltung zum Thema Cyber Security. Wir nennen sie „Command Control. The Leading Summit for Cyber Security“.

Es ist wohl sehr schwierig, IT-Lösungen auszustellen, speziell im Security-Bereich?

In der Tat. Eine Messe wird diesem Thema nicht gerecht. Wir haben den Anspruch, den Entscheidern Entscheidungshilfe zum Thema Cyber Security zu geben. Das geschieht z. B. dadurch, dass die einzelnen Aspekte der Cyber Security in Szenarien visualisiert werden.

Wir haben dazu viele neue Ideen. Es wird dann natürlich auch Key-Notes, Workshops und One-to-One-Meetings geben: Also

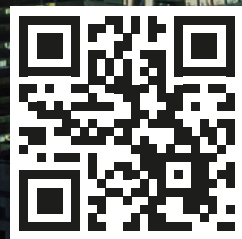


metafinanz
Business & IT Consulting

We. Ensure. Success.

Starte Deine Reise in die digitale Zukunft.

Vielfalt. Menschlichkeit. Mitgestaltung. Zukunftsfähigkeit.
Wir transformieren das Business unserer Kunden in neue Modelle für die Wirtschaft 4.0. Als Unternehmen der Allianz Gruppe vereinen wir die Vorteile des Konzernumfelds mit einer lebendigen StartUp-Kultur unter einem Dach. Wir suchen Mitarbeiter, die mit Leidenschaft gestalten und bereit sind, Verantwortung zu übernehmen. Sei dabei!



www.metafinanz.de



Digital werden die individuellen Maße für eine Jacke eingegeben und das maßgeschneiderte Kleidungsstück wird angezeigt.



E-Tankstelle: Die Messe München bietet für ihre Kunden kostenlose Elektroladestationen für E-Autos an. Bis Ende des Jahres werden es rund 50 Ladestationen im Parkhaus und auf dem Gelände.

verschiedene Formate, um die Informationen so aufzubereiten, dass diejenigen, die die Entscheidung dann treffen und nicht zwangsläufig auch IT-Experten sind, sich aus dem Menü aus Informationsmöglichkeiten das Beste für ihr Unternehmen auswählen können. Der Summit soll auf europäischem Level sein, also weit über Deutschland hinausreichen.

Ist Ihre Arbeit dadurch wieder kreativer geworden? Weil Sie sich überlegen müssen, wie man etwas Virtuelles analog darstellt?

Definitiv. Das klassische, alte Messegeschäft bestand darin – vereinfacht und banal gesprochen – Quadratmeter Ausstellungsfläche zu verkaufen. Jetzt sind wir natürlich sehr viel mehr gefordert, mit den

Ausstellern gemeinsam solche Szenarien zu entwickeln. Die Anforderung wird dadurch größer, aber die Aufgabe auch kreativer. Das Ganze macht dadurch auch mehr Spaß.

Sie waren eben erst in Austin. Welche Inputs haben Sie von dort mitgenommen?

Mit unserer „Innovation Journey“ zur South by Southwest (SXSW) haben wir für unsere Partner und Kunden ein Format geschaffen, das in Austin zum zweiten Mal zum Einsatz kam. Die Journey-Teilnehmer gehen auf die Reise und werden dabei inhaltlich von einem Content-Team begleitet. Bei der ersten Reise 2017 war das innerhalb Münchens, bei der zweiten sind wir nach Austin geflogen. Die dritte ist im Juni zu unserer Leitmesse automatica in München.

Employer Branding

Beim Employer Branding handelt es sich um ein Set von Marketing-Maßnahmen, das darauf abzielt, ein Unternehmen als interessanten und guten Arbeitgeber zu positionieren.

In Austin bot die SXSW eine umfassende Einordnung von Zukunftsthemen. Die Themen von Blockchain über AI bis hin zu Smart Mobility (inklusive der Diskussion über ein Leben auf dem Mars) wurden ausgiebiger diskutiert als in Europa oder auf ähnlichen Konferenzen üblich. Bei dieser mehrtägigen Reise nach Austin schufen wir zudem ein bayerisches Innovation Village, in dem die Teilnehmer die Möglichkeit hatten, das Erlebte zu reflektieren und Ideen zu vertiefen. Ein Tenor der SXSW ist, dass die Treiber von Innovation nicht darauf warten sollen, dass jemand anderer die Idee umsetzen möchte. Sondern dass du selbst die Veränderung beginnen musst.

Sollen auch Mitarbeiter im Unternehmen, die nicht in einer Führungsposition sind, selbst mit Veränderungen beginnen?

Wir haben gerade eine Aktion gestartet, die nennt sich „The Big Scrub.“ Dabei sind Mitarbeiter aufgefordert, Prozesse, Regeln und Formulare zu melden, die sie besonders in ihrer Arbeit behindern. Nach dem Ablauf von 14 Tagen kommt es dann zur Abstimmung. Die Prozesse, Regeln oder Formulare, die am meisten Stimmen bekommen, werden überprüft und dann entweder vereinfacht, digital abgewickelt oder ganz abgeschafft. So können sich alle Mitarbeiter aktiv einbringen.

In welcher Form haben digitale Anwendungen das Messewesen bereits transformiert? Werden die digitalen Potenziale bei der Messe München zur Gänze ausgenutzt oder gibt es noch Nachholbedarf?

Es gibt bei der Messe München bereits zahlreiche digitale Anwendungen. Wir digitalisieren unsere Prozesse, Abläufe und die Infrastruktur und wir bieten digitale Produkte und Services. Dazu gehören interaktive Hallenpläne, digitale Ausstellerverzeichnisse, ein Webshop, das kostenlose WLAN und neue Registrierungs- und Einlasssysteme. Auch mit modernen CRM- oder Finanz- und Planungssystemen verbessern wir Prozesse für unsere Kunden. Darüber hinaus bieten wir digitale Produkte und Services, mit denen wir Umsatz generieren wie die

Open-Innovation-Plattform bei der ISPO oder zahlreiche Service-Apps.

Seit 2010 hat die Messe München Profit erwirtschaftet, trotz Schuldentilgung. Wie viel Umsatz haben Sie im Jahr 2017 gemacht?

2017 war ein erfolgreiches Messejahr: Der Umsatz lag bei 332,6 Millionen Euro. Im Rekordjahr 2016 – in einem Jahr mit der Weltleitmesse bauma – waren es 428 Millionen: Damit gehören wir weltweit zu den Top Ten und zu den bedeutendsten Messeveranstaltern.

Die Messe nützt auch der Stadt München und der ganzen Region: In einem normalen Messejahr lösen wir außerhalb unserer Messe eine Umwegrentabilität von 2,6 Milliarden Euro aus. Das verdienen Hoteliers, Gastronomen, Taxifahrer, Handwerker oder Händler.

Haben diese positiven finanziellen Entwicklungen etwas mit der Digitalisierung zu tun?

Auch. Mit dem 2017 neu gegründeten Geschäftsbereich Digital haben wir uns das Ziel gesetzt, bis 2021 fünf Prozent des Umsatzes aus digitalen Produkten und Services zu erzielen.

Sie wachsen schneller als die anderen deutschen Messestandorte. Was ist Ihr Erfolgsrezept?

Unser Dreischritt: Festigung des Heimatmarktes, Wachstum im Ausland und Digitalisierung. Wir gehen gezielt vor und konzentrieren uns auf die wichtigsten Wachstumsmärkte. Außerdem haben wir ein weltweites Netzwerk mit mehr als 70 Auslandsvertretungen. Wir haben auch mehrere Auslandsstöchter, mit denen wir Veranstaltungen im Ausland durchführen. Da sind wir auch in Märkten, die in Sachen Digitalisierung sogar weiter sind als wir. Es ist also nicht so, dass wir von München aus sagen würden: „Wir beglücken jetzt die Welt!“, sondern wir lernen auch viel aus diesen Märkten, in denen wir präsent sind.

Sie sind viel in China tätig. Was kann man speziell aus diesem Markt lernen?

China ist in manchen Bereichen viel digitaler als wir. Bei den Messen dort wird nichts mehr auf Papier gedruckt, die Besucherwerbung läuft ausschließlich online. Über Wechat werden Zahlungen abgewickelt,

Urlaube gebucht und Bestellungen aufgegeben. Natürlich hat das Thema Datenschutz in China eine viel geringere Bedeutung als bei uns. Man muss auch nicht alles eins zu eins übernehmen, aber ich finde schon, dass man dort eine Menge lernen kann.

Wie wirkt sich die Digitalisierung auf das Erlebnis der Besucher auf der Messe aus?

Sehr positiv. Die Digitalisierung erleichtert viele Dinge: mit dem Buchen eines elektronischen Besuchertickets, mit Match-Making-Services, mit digitalen Hallenplänen oder praktischen Apps. Der Messebesuch kann schon im Vorfeld exakt geplant werden. Die meisten Besucher kommen nicht mehr unvorbereitet auf die Messe so wie früher, sondern sie sehen sich die Ausstellungsstände im Online-Ausstellungsverzeichnis an und machen daraufhin gezielt ihre Verabredungen aus. Der Teilnehmer kann auch nach der Messe noch Files und

„Wir haben über drei Millionen Besucherdaten. Mithilfe von künstlicher Intelligenz können wir dadurch beispielsweise neue Marketingkonzepte oder neue Produkte entwickeln.“

Inhalte downloaden, die er vor Ort vielleicht verpasst hat. Früher ging man auf eine Messe, um andere Menschen zu treffen; heute erwarten die Besucher mehr, sie wollen sich digital vernetzen, Ideen austauschen, nicht nur für ein paar Messtage, sondern das ganze Jahr über.

Werden Messen im Zeitalter der Digitalisierung wichtiger oder werden sie Ihrer Meinung nach durch digitale Möglichkeiten im Internet teilweise oder in näherer Zukunft ersetzt?

Es geht heute nicht um die Entscheidung zwischen Messe oder digitaler Plattform. Sondern es geht darum, wie sich Messen und digitale Welt am besten ergänzen können. Messen müssen sich die Digitalisierung zu Nutzen machen. Aber die Face-to-Face-Kommunikation wird auch das Internet nicht ersetzen können. So erleben wir die umgekehrte Situation: Trotz Internet nimmt die Zahl der Aussteller und Besucher auf unseren Veranstaltungen zu.



Reverse Mentoring: Eine junge Mitarbeiterin unterstützt Messechef Klaus Dittrich bei seinen Social-Media-Aktivitäten.

Und: Die Zahl der Kunden aus dem Ausland steigt kontinuierlich an. Wir haben inzwischen Veranstaltungen mit mehr als 50 Prozent Ausstellern und Besuchern aus dem Ausland. Man kann also sagen, dass das Umfeld einer Messe digital angereichert worden ist, aber die persönliche Begegnung ist nach wie vor unersetzlich.

Stichwort IoT: Gibt es bei Ihnen eine IoT-Messe? Spielt IoT für die Messe München eine große Rolle?

Wir haben keine spezielle Messe für das Internet of Things. Aber das Internet der Dinge spielt auf vielen unserer Veranstaltungen eine große Rolle.

Was sind für Sie die spannendsten Zukunftstrends?

Spannende Zukunftstrends sind zum Beispiel digitale Schaufenster, mit denen sich Aussteller präsentieren können. Ein sehr weites Zukunftsfeld ist Artificial Intelligence (AI), die künstliche Intelligenz. Mit ihr können riesige Datenmengen schnell ausgewertet werden, Computerergebnisse können menschliche Entscheidungen beschleunigen und präzisieren. Wir sitzen ja

CRM – Customer-Relationship-Management

Beim CRM, auf Deutsch „Kundenbeziehungsmanagement“, geht es um das Systematisieren der Kundenbeziehungen. Mit einem CRM-System lässt sich der ganze Verlauf der Kundeninteraktion verfolgen: Anrufe, E-Mails, Beschwerden, Meetings, Abschlüsse etc. Dies lässt sich zu Marketingzwecken auswerten und erlaubt, die Servicequalität zu verbessern. Ferner können weitere potenzielle Kunden identifiziert werden.

auf einem großen Datenschatz: Wir haben über drei Millionen Besucherdaten. Mithilfe von künstlicher Intelligenz können wir dadurch beispielsweise neue Marketingkonzepte oder neue Produkte entwickeln.

Sind Messen durch die neuen digitalen Lösungen weniger personalintensiv? Nein. Digitalisierung bedeutet ja auch den Versuch, die Prozesse, die Abläufe und die Infrastruktur zu digitalisieren. Da gibt es eigentlich keine großen Einspareffekte beim Personal, weil sich dann eben neue Felder auftun. Wir haben jetzt also nicht Personal reduziert, sondern im Gegenteil eher Personal aufgebracht.

Welche Entscheidungen zur Digitalisierung der Messe München haben sich im Nachhinein als höchst sinnvoll und welche als erfolglos herausgestellt? Zwei Entscheidungen sind besonders sinnvoll: die Gründung des Geschäftsbereichs Digital – mit dem Zugeständnis weitgehender Freiräume und neuer Arbeitsstile an die neuen Kollegen – und das Reverse-Mentoring-Programm.

Was immer noch eine Herausforderung darstellt ist unser Webshop, den wir über drei Jahre lang entwickelt haben. In dem kann jedes Produkt, das es im Umfang einer Messe auch von all unseren Dienstleistern zu bestellen gibt, online gebucht werden. Am Ende steht der Kunde davor und ist völlig überfordert.

Das ist in etwa so, als wenn Sie ein Auto bestellen würden und sich jede Radmutter sowie jede Felge in hundert verschiedenen Varianten zusammenstellen können. Wir sind jetzt dabei, dem Kunden Pakete anzubieten, zu denen er zusätzlich etwas buchen kann. Speziell bei der Reise ins Silicon Valley haben wir gelernt, den Kunden so früh wie irgend möglich bei der Entwicklung neuer Produkte einzubinden.

Sie haben gesagt, dass Sie eine Messe nicht vom Schreibtisch aus erledigen könnten. Wieso ist es so wichtig, dass Sie mitten im Geschehen sind? Weil die persönliche Begegnung und der direkte Austausch immer noch die entscheidenden Faktoren sind. Reale Messen und das direkte Gespräch sind immer wieder faszinierend. Und sie sind

ein Seismograph für Entwicklungen. Das erfahren sie nicht am Schreibtisch. Früher waren die Rollen in unseren Beziehungen vorgezeichnet, heute müssen diese permanent neu definiert und verhandelt werden.

Nachhaltigkeit – auch in Kombination mit der Digitalisierung – ist ein wichtiger Unternehmenswert der Messe München. An welchen Projekten kann man das erkennen?

Unsere Photovoltaik-Anlage gehört weltweit zu den größten Anlagen auf Dächern. Von dort werden auch unsere bald 50 Ladestationen für Elektroautos auf unserem Gelände versorgt. Als vorbildlich gilt auch unsere Geothermie. Wir sind die einzige Messengesellschaft in Europa, die Erdwärme nutzt.

Hat sich in den letzten 20 Jahren die inhaltliche Ausrichtung der Messen inhaltlich digitaler geworden? Erwarten Sie, dass der Trend sich in Zukunft noch stark wandeln wird?

Eindeutig, ja. Internet, Videos, Animationen gehören heute dazu. Und der Einsatz von VR-Brillen bei einer ISPO oder bauma

eröffnet völlig neue Sicht- und Erlebnismöglichkeiten. Eine wichtige Veränderung in den letzten 20 Jahren ist: Die Präsentationsflächen für Produkte wurden kleiner und die Kommunikationsflächen für Kunden umso größer. Mit dem Kunden zu interagieren, ist daher wichtiger, als das Produkt selber zu zeigen. Ein Beispiel: Adidas war jetzt seit elf Jahren zum ersten Mal wieder auf der ISPO – mit keinem einzigen Produkt! Sie haben nämlich eigene Showrooms, in die sie ihre Kunden einladen, um ihre Kollektionen zu zeigen. Was sie aber auf der ISPO gezeigt haben, sind ihre digitalen Lösungen. Das

tiger, als das Produkt selber zu zeigen. Ein Beispiel: Adidas war jetzt seit elf Jahren zum ersten Mal wieder auf der ISPO – mit keinem einzigen Produkt! Sie haben nämlich eigene Showrooms, in die sie ihre Kunden einladen, um ihre Kollektionen zu zeigen. Was sie aber auf der ISPO gezeigt haben, sind ihre digitalen Lösungen. Das



Klaus Dittrich im Gespräch mit Florentina Hofbauer.

Florentina Hofbauer

Fotos: Messe München

beginnt schon bei der Produktentwicklung. Hier wird versucht, den Kunden möglichst früh in das Design des Produktes miteinzubeziehen. Wichtig ist auch die Fertigung am Point of Sale: Das Stichwort hierbei ist „Speed-Factory“.

Was ist eine Speed-Factory?

Bis früher ein neuer Trend aus Amerika nach Europa kam, hat das ein oder zwei Jahre gedauert, heute ist es dank Social Media eine Sache von Wochen. Ein großer Player wie Adidas reagiert darauf, indem er an den Hotspots der Welt, dort wo Trends entstehen, ganz nah beim Kunden sein will. Diese Hotspots sind etwa London, Paris, Shanghai oder New York. Das Ziel hierbei ist, das Produkt am Verkaufspunkt zu fertigen. Dort gibt es dann die Möglichkeit, Schuhe nach den Wünschen des Kunden zu produzieren, sodass er das gewünschte Design bestellt und eine Stunde später abholen kann. Adidas hat auf der ISPO weder Schuhe noch Trikots gezeigt, sondern digitale Lösungen und der Stand wurde überrannt!

Wird die Face-to-Face-Kommunikation am Ausstellungsstand deshalb wieder wichtiger?

Es war immer wichtig. Besonders interessant war in diesem Zusammenhang die Diskussion in München, als Mitte der neunziger Jahre die Frage aufkam, ob man im Zeitalter des Internets überhaupt noch ein neues Messegelände bauen sollte. Die Standarddiskussion war, ob man in zehn oder 20 Jahren Messen noch brauchen wird. Ich glaube, dass diese Frage heute beantwortet ist: Man muss die persönliche Kommunikation pflegen. Die ist auch durch Internettelefonie nicht ersetzbar. Das zeigen auch ganz interessante Beispiele: Zalando ist ein reiner Onlinehändler, der kürzlich die Messe Bread & Butter gekauft hat. Oder Amazon macht einen Buchladen auf und die Leute stehen Schlange, weil sie die ersten sein wollen, die im Amazon-Buchladen stehen. Xing organisiert Stammtische! Das zeigt ja: Digital allein ist es nicht. Es ist bereichernd und erweiternd, aber die persönliche Kommunikation ist nicht ersetzbar und das ist unser Kerngeschäft. Denn eines wird bleiben: Sie sehen auf Messen heute das, was morgen unser Leben verändert.

Organisationsrebellien: Veränderung braucht Störung

Marcus Raitner arbeitet als Agile Transformation Agent und Agile Coach bei der BMW Group IT. In seinem Blog „Führung erfahren!“ schreibt er seit über sieben Jahren über die Themen Führung, Agilität, neue Arbeit, Digitalisierung und vieles mehr.



Aristoteles schrieb einst: „Ein ein guter Mensch ist nicht immer ein guter Bürger.“ Entsprechend ist ein guter Mitarbeiter nicht immer ein angepasster Mitarbeiter. Organisationsrebellien sorgen für Störung und halten die Organisationen damit lebendig.

Der zivile Ungehorsam ist eine Form des Widerstands innerhalb einer bestehenden Ordnung. Er lehnt die bestehenden Strukturen nicht ab und zielt nicht auf eine Auflösung des Systems. Wer zivilen Ungehorsam übt, stellt sich nicht außerhalb der Ordnung, sondern nimmt ganz bewusst eine Bestrafung seines öffentlich zelebrierten Ungehorsams in Kauf. Bekannt wurde der Begriff durch das Essay „On the Duty of Civil Disobedience“ von Henry David Thoreau, in dem er erklärte, warum er aus Protest gegen den Krieg gegen Mexiko und die Sklavenshaltung keine Steuern mehr bezahlte.

Den redlichen Bürger zeichnet also gerade nicht absoluter Gehorsam aus, sondern ein qualifizierter Rechtsgehorsam (Jürgen Habermas). Das schließt den Widerstand in Form zivilen Ungehorsams ein. Daraus resultiert auch der moralische Auftrag für Organisationsrebellien. Ihr Regelbruch ist nie gegen die Organisation gerichtet, sondern als Beitrag zu ihrer Verbesserung zu verstehen. Organisationsrebellien identifizieren sich mit der Organisation und ihrem eigentlichen Zweck, aber nicht mit allen damit nicht kohärenten Regeln oder einer als hinderlich empfundenen Organisationskultur. Ihr Regelbruch ist die notwendige Störung, um die Organisation vor Selbstgefälligkeit und Trägheit zu bewahren.

Gifford Pinchot III stellte 1986 in seinem Buch „Intrapreneuring: Why You Don't Have to Leave the Corporation to Become an Entrepreneur“ zehn Gebote für Intrapreneure auf. Angelehnt daran und angereichert mit einer Prise Working Out Loud und Effectuation halte ich die folgenden Prinzipien für das Wirken von Organisationsrebellien für wichtig:

1. Seid mutig – seid radikal. Kommt jeden Tag mit der Bereitschaft zur Arbeit, gefeuert zu werden.
2. Habt eine große Vision und klare Prinzipien, die euch leiten.
3. Fokussiert euch auf die nächsten konkreten Schritte, die ihr hier und heute unabhängig von eurer Stellen-

beschreibung unternehmen könnt, um eurer Vision näherzukommen.

4. Findet Verbündete, vernetzt euch und werdet eine Bewegung.
5. Umgeht Regeln und Anordnungen, um ein Ziel zu erreichen, aber nie zum Selbstzweck.
6. Arbeitet solange wie möglich im Untergrund – zu viel Sichtbarkeit zu früh weckt das Immunsystem der Organisation.
7. Seid dankbar für Unterstützung.
8. Lernt aus Widerstand und Niederlagen.
9. Seid beharrlich im Bemühen und bescheiden in der Erfolgserwartung. (Götz W. Werner)
10. Handelt stets zum Wohle der Organisation und ihrer Kunden.

Wer als Führungskraft Rebellen fördern will, braucht eine Kultur, in der Vielfalt und Dissens gut gedeihen. Es braucht einen geschützten Raum, in dem der Status quo hinterfragt werden darf. Im Dschungel der Politik in der Organisation gibt es genügend Fallstricke, die eine sofortige Immunreaktion des Systems auslösen. Diese Fallstricke zu erkennen und zu vermeiden und so seine Rebellen zu beschützen, ist Aufgabe der Führungskraft. Und macht sie damit selbst zum Rebellen.

Richtig gut wird es, wenn nicht nur wenige auserwählte Rebellen diesen Freiraum zum Hinterfragen des Status quo haben, sondern möglichst viele, sodass die rebellischen Ideen auf positive Resonanz treffen können. Eine wesentliche Führungsaufgabe ist es daher, diesen Freiraum zu schaffen durch konsequente Fokussierung auf das Wesentliche und eine Kultur der Nachhaltigkeit, in der Beschäftigte nicht mit Produktivität verwechselt wird.

Je länger man nun über diese Aufgaben nachdenkt, desto mehr erkennt man, dass das alles eigentlich gar nicht so viel mit Rebellen zu tun hat. Jeder Mitarbeiter sollte den Freiraum haben, sich auszuprobieren und zu lernen, ohne in den Mühlen der Politik unterzugehen. Jeder sollte den Freiraum haben, über den Tellerrand zu schauen und den Status quo zu hinterfragen. Und jeder sollte ermächtigt und ermutigt werden, davon auch Gebrauch zu machen.

Dr. Marcus Raitner

Foto: privat

1. INTERNET OF THINGS (IOT)

Das Internet der Dinge bzw. Internet of Things (kurz IoT) erlebt seit Jahren einen regelrechten Boom, der sich sowohl auf technologischer als auch auf betriebswirtschaftlicher Ebene abspielt. Diese Entwicklung ist Teil des aktuell stattfindenden technologischen Wandels in einer immer stärker vernetzten und digitalen Welt. So verbergen sich unter dem Sammelbegriff IoT eine Vielzahl an Technologien und konkrete Anwendungen. Bekannte Beispiele finden sich in den Kategorien Smart Home bzw. Smart City, im Automotive-Bereich oder im sogenannten Industrial IoT.

Das Internet der Dinge bezeichnet allgemein die Verknüpfung eines physischen Objekts bzw. Gegenstands (thing) mit einer digitalen Repräsentation in einer vernetzten Struktur, die dem Internet ähnlich ist. Man kann sich also vorstellen, dass ein solch generischer Begriff viel Raum zur Interpretation lässt und nur schwer abgegrenzt werden kann. Die Übergänge sind meist fließend und die Art der Betrachtung auf dieses hoch spannende Themenfeld ist vielseitig.

So stellen sich aus technischer Sicht Fragestellungen bzgl. Datenmanagement und Datensicherheit, da im Internet der Dinge eine Vielzahl sensibler Daten aus der physischen Welt erhoben und ausgetauscht werden. Betriebswirtschaftliche Überlegungen beleuchten hingegen die Chancen und Risiken von IoT-Lösungen und zeigen Strategien für Unternehmen, um mittels IoT fit für die Zukunft zu werden. Das Internet of Things wird aber auch kritisch betrachtet. So wird der aktuelle Hype hinterfragt und mögliche Auswirkungen auf Unternehmen und Gesellschaft analysiert.

Im Folgenden werden neben Herausforderungen der digitalen Vernetzung und zahlreichen praktischen Anwendungen auch allgemeine, sowie sicherheitsrelevante IoT-Themen vorgestellt.

MEIST GEKLIKT – Unsere erfolgreichsten Blog-Beiträge

Unsere Beiträge wurden insgesamt **147.031** Mal geklickt*

Beiträge zum Thema **BLOCKCHAIN** erhielten **32.806** Klicks.

	Autor Thema
#1	Dr. Nils Daecke Internet of Things – Game Changer oder Gadget? Seite 28
#2	Nigel Stanley IoT-Geräte: Wenn Cyber Security für Kunde und Marke zum kritischen Faktor wird Seite 49
#3	Falk Senger IoT-Plattformen sind Voraussetzung für Industrie 4.0 Seite 80
#4	Steffen Krotzsch Das Internet der Dinge im Versicherungsbereich Seite 77
#5	Felix Heimbrecht IoT und AI: Eine Co-Evolution Seite 32

*Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 01. August 2017 – 02. Mai 2018.

1.1 ALLGEMEIN	
1.1.1 Kritische Auseinandersetzung	
Donald Wachs IoT – realer Hype oder eine neue Blase?	26
Dr. Nils Daecke Internet of Things – Game Changer oder Gadget?	28
Axel Godoy Sind deutsche Unternehmen bereit für IoT?	30
Felix Heimbrecht IoT und AI: eine Co-Evolution	32
1.1.2 Strategien	
Dr. Thomas Zander „Industrial Internet of Things“-Lösungen helfen uns allen – wenn die Anbieter ihre Hausaufgaben machen	34
Harald A. Summa Die drei Ausprägungen des IoT und was wir dafür tun können, dass unsere digitale Zukunft eine gute Zukunft wird	35
Christoph Henkels NarrowBand IoT – der schlanke Einstieg ins Internet der Dinge	37
Andreas Odenkirchen Industrial Internet of Things (IIoT): Darauf kommt es an	39
Klaus Jaworski Virtual Reality – Science Fiction von heute	41
Sascha Hellermann Mit Blockchain-Technologie bereit für das Internet of Things	42
1.1.3 Visionen	
Dr. Thomas Endres IoT – eine große Chance für Europa	43
Georg Goller Der Weg zur digitalen Transformation	45
Michaela Tiedemann Warum künstliche Intelligenz dem Internet of Things zum Durchbruch verhelfen wird	46
1.2 SICHERHEIT	
1.2.1 Herausforderungen	
Markus Reiniger Internet of Things (IoT) – von der Zukunft von Endgeräten bis hin zu ihren Sicherheitsproblemen	47
Nigel Stanley IoT-Geräte: Wenn Cyber Security für Kunde und Marke zum kritischen Faktor wird	49
Claus Vaupel Sicherheitsrisiko Internet of Things	50
Nicolas Ehrschwendner Datenverlust lauert auch im IoT	51
1.2.2 Ansätze und Lösungen	
Jan Junker Hackers Paradise – Sicherheit im Internet of Things	52
Claas Lorenz IoT: Risikomanagement nur mit Security by Design	53
Wilfried Kirsch Internet der Dinge: Security Guidelines	54
1.3 DIGITALE VERNETZUNG	
1.3.1 Datenmanagement	
Robert Romanski Datenexplosion: wirtschaftliches Management und Hochverfügbarkeit dank Hyperscale-Rechenzentren	56
Carsten Hochschon Datenübertragung mittels Blockchain	57
1.3.2 Auswirkungen	
Dr.-Ing. Darko Sucic Vernetzt denken und handeln	59
Jochen Busch Ein neues Netz als Herzstück für intelligente Städte	60
Florian Hermsdorf Das Internet wird unsichtbar	61
Henning Neu I(di)IoT – wie Smart Devices unserer Gesellschaft Innovation vorgaukeln und unseren Alltag komplexer machen	62
Manfred Klaus Warum das „Internet der Dinge“ in den Marketingplan gehört	64
Alexander Eser Internet of Things (IoT) und unser Zuhause – durch Artificial Intelligence (AI) wird der Zero Click Sale möglich	65
Kurt Kapp IoT – neue Handlungsfelder für die Landeshauptstadt München	67
Markus Reichenberger IoT im Zusammenhang von Interoperabilität, Echtzeitanwendungen, Architekturen und sozialer Akzeptanz	69
1.4. IOT IN DER PRAXIS	
1.4.1 Business IoT	
Dr. Thomas Lücking Vom Produkt zum Service – organisatorischer Wandel als Voraussetzung für erfolgreiche IoT-Lösungen	71
Hanna Pradler Wie IoT-Geräte für Konsumenten nützlicher werden	74
Math Huntjens Die smarte Brücke zwischen Produktion und Office	75
Christian Haas Am Ende gewinnt immer der Kunde ...	76
Steffen Krotzsch Das Internet der Dinge im Versicherungsbereich	77
1.4.2 Industrial IoT	
Dr. Andreas Leupold Industrial Internet of Things (IIoT): rechtlicher Handlungsbedarf für Unternehmen	78
Falk Senger IoT-Plattformen sind Voraussetzung für Industrie 4.0	80
Uwe Weber Industrial Internet of Things: wie der Fertigungsablauf mittels Edge Computing intelligent gesteuert wird	82
Tim Kappler Die flächendeckende Anwendung von IoT-Geräten in Industrie-Unternehmen – eine Bestandsaufnahme aus Sicht der Rückversicherung	83

1.1 ALLGEMEIN

1.1.1 Kritische Auseinandersetzung

IoT – realer Hype oder eine neue Blase?

Die Digitalisierung schreitet mit großen Schritten voran. Wir sehen an den Beispielen von unserem Partner GE und vielen unserer Kunden, wie innovative Vorreiter die digitale Agenda definieren und umsetzen. Das Potential der Digitalisierung und die Auswirkung auf die neuen, teilweise disruptiven Geschäftsmodelle, lässt sich nach heutigem Stand nur erahnen. Unsere Kunden müssen sich der Tatsache stellen, dass die technologische Umwälzung nicht mehr aufzuhalten ist. Um im Markt zu bestehen, müssen die notwendigen Kenntnisse und Fähigkeiten aufgebaut werden, um die Herausforderungen der Digitalisierung anzugehen.

Das Internet der Dinge (kurz IoT aus dem englischen Internet of Things) stellt in der industriellen Digitalisierung ein zentrales Element dar. Hier hat sich auch der Begriff IIoT (Industrial Internet of Things) etabliert. Im weitesten Sinne wird IoT als computergestützte Vernetzung der physikalischen (u.a. Maschinen, Produkte, Sensoren) mit der virtuellen (u.a. Daten, Software) Welt über das Internet verstanden, die eine Zusammenarbeit der Objekte (things) ohne menschliche Interaktion ermöglicht.

Im Kern unterteilen wir IoT in die Evolutionsstufen Get Connected, Get Insights und Get Optimized. Get Connected beschäftigt sich dabei mit der Vernetzung und Automatisierung, Get Insights mit der Informationsgewinnung aus den gewonnenen Daten mit Hilfe von Algorithmen und Machine Learning und Get Optimized umfasst die Veredelung der gewonnenen Informationen im Sinne von Kosteneffizienzsteigerungen oder Umsatzpotentialaufdeckungen durch neue Business Modelle.

Das Zusammenspiel der genannten Evolutionsstufen können wir anhand eines einfachen Beispiels aus dem „Smart Factory“ Umfeld verdeutlichen. In der Smart Factory sind verarbeitende Maschinen und auch die Produkte vernetzt und in das Netzwerk von Informationen eingebunden. Die Produkte tragen eine Markierung, die die Informationen beinhaltet, welche Bearbeitungsschritte mit den passenden Parametern für sie ausgeführt werden müssen (Get Connected). Algorithmen an den Maschinen helfen Entscheidungen in Echtzeit zu treffen, wie z.B. welche Maschine als nächstes angesteuert werden muss. So kann eine Maschine umgangen werden, die zum

Beispiel durch ein fehlerhaftes Teil blockiert ist (Get Insights). Die Maschinendaten können auch dazu genutzt werden die sogenannte Downtime, die Zeit in der eine Maschine repariert oder gewartet wird, maßgeblich zu reduzieren. Der Kunde kann dann einen Service erwerben, der es ihm ermöglicht den Fortschritt der Produkterstellung über eine für ihn zur Verfügung gestellte Applikation zu verfolgen und bis zur letzten Minute noch Änderungen zu realisieren (Get Optimized).

Get Connected

BearingPoint hat in den letzten Jahrzehnten vielen Unternehmen dabei geholfen, ihre internen Prozesse weitgehend zu automatisieren, sowie die Prozessharmonisierung und Standardisierungen als Grundvoraussetzungen für die Automatisierung vorzubereiten. Mit den Möglichkeiten des IoT bieten sich nun aber noch mehr Möglichkeiten, u.a. mit komplexen Maschinen zu interagieren und kleinste Produkte zu vernetzen.

Als größte Herausforderungen im Bereich Get Connected wurden in den letzten Jahren fehlende Standardisierung, Cyber Security und noch nicht ausgereifte Technologien angesehen.

Notwendige Standardisierungen in den Schnittstellen und Kommunikationsprozessen sind mittlerweile über diverse Institute und Konsortien auf dem Weg gebracht worden – beispielhaft sollen hier die OPC Foundation (<https://opcfoundation.org>) oder die Open Connectivity Foundation (kurz OCI; <https://openconnectivity.org/>) erwähnt werden. Auch hinsichtlich Cyber Security gibt es diverse Aktivitäten, um die Sicherheit der IoT Objekte erheblich zu verbessern. Neben der auch hier starken Open Source Fraktion (Open Web Application Security Project (OWASP); <https://www.owasp.org>), sind auch diverse staatliche Instanzen sehr stark aktiv - beispielhaft hier erwähnt der vom U.S. Senat eingeführte „Internet of Things Cybersecurity Improvement Act of 2017“ (<https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt>).

In Bezug auf technologische Verbesserungen kann auf die unterschiedlichsten Technologien für drahtlose Datenübertragung verwiesen werden. Low-Power-Wide-Area (kurz LPWA) oder Long Range (kurz LORA) Technologien sind relative neue Elemente von Verbindungstechnologien für geringe Reichweite. Mit der anstehenden 5G Technologie für mobile Datenübertragung für große Reichweiten und der durchgehenden Einführung des IPv6 Standards stehen neue Meilensteine bevor, die eine Verbreitung der IoT Innovationen maßgeblich vorantreiben werden.

Zusammenfassend kann für den Bereich Get Connected festgestellt werden, dass die Grundelemente für die Vernetzung bereits vorhanden sind

und die Herausforderungen mit großer Geschwindigkeit angegangen werden.

Get Insights

Betrachten wir die Evolutionsstufe Get Insights stellen wir auch hier fest, dass durch die kostengünstige Cloud basierte Datenhaltung und distributive Datenprozessierung (geprägt durch die Hadoop Technologie der Apache Foundation (<http://hadoop.apache.org/>)) Meilensteine in der Datenverarbeitung von Massendaten – auch BigData genannt – erreicht wurden und bereits überall im Einsatz sind. Für die im IoT Bereich vorwiegende Verarbeitung von diskreten Realtime Daten die mittels Sensoren erzeugt, und auch als Datenströme oder Datastreams bezeichnet werden, sind diverse durch die Apache Foundation unterstützte Erweiterungsprojekte im Umlauf (u.a. Apache Flink, Apache Storm).

Neben den starken Open Source Fraktionen sind diverse kommerzielle Angebote, die sich an Hadoop anlehnen oder diese Technologien nutzen auf dem Markt (u.a. Amazon WebServices, Microsoft Azure Plattform). Aufbauend auf diesen Technologien können durch sogenannte Data Scientists Algorithmen entwickelt werden, welche die Massendaten verarbeiten und neue Erkenntnisse aus diesen gewinnen – eine Technologie die noch vor einigen Jahren als nicht umsetzbar eingestuft wurde. Unsere Lösung HyperCube (<https://www.hcube.io/en/>) ist ein sehr gutes Beispiel wie Tools Unternehmen dabei helfen den Mehrwert aus den Daten zu generieren. Machine Learning ist in vielen Bereichen schon längst im Einsatz (z.B. Einsatz von Bots für sich wiederholende Aufgaben im Customer Service, computergesteuerte Sprachenprozessierung mit Siri oder Amazon Echo) und steht auch im industriellen Umfeld vor dem Siegeszug.

Eine weitere interessante Technologie aus dem IoT Bereich ist unter dem Namen Edge Analytics bekannt geworden (auch Complex Event Processing kurz CEP genannt). Dabei werden die Algorithmen nicht erst in der Cloud ausgeführt, sondern direkt vor Ort an den Maschinen oder Produkten, also auf den Micro Controllern die direkt mit den Maschinen verbunden sind. Diese Miniatur Computer werden auch als Edge Devices bezeichnet. Diese Technologie wird u.a. dafür eingesetzt, um sehr zeitnahe Entscheidungen zu treffen oder mit Hilfe von Algorithmen das übertragene Datenvolumen in die Cloud zu reduzieren.

Aktuell sehen wir sogar, dass speziell für Machine Learning ausgelegte Prozessoren für den Edge im Konsumerbereich eingeführt werden (u.a. Tensor Processing Units (TPUs) von google, <https://cloud.google.com/blog/big-data/2017/05/an-in-depth-look-at-googles-first-tensor-processing-unit-tpu>; oder

Huawei's Kirin Chips <http://www.zeit.de/digital/mobil/2017-09/ifa-huawei-richard-yu-kirin-970-kunstliche-intelligenz>). Wir sind uns sicher, dass diese Technologien auch bald in IoT Edge Computing Einzug erhalten werden.

Zusammenfassend können wir für den Bereich Get Insights festhalten, dass die Technologien, um aus den IoT Objektdaten Informationen zu gewinnen, sehr weit fortgeschritten sind. Es fehlt allerdings an Experten und Know-how in den Unternehmen, um die bereits vorhandenen Technologien effizient auszunutzen.

Get Optimized

Jegliche Vernetzung und das aus den Daten generierte Wissen ist jedoch nicht zu verwenden, wenn daraus keine Vorteile für den Kunden entstehen.

In der Evolutionsstufe Get Optimized werden daher alle Themen zusammengefasst, die Optimierungen und Effizienzsteigerungen der vorigen Prozesse behandeln. Dadurch, dass die Potentiale hier noch gar nicht voll erfasst werden können, fällt es jedoch schwer hier so konkret wie in den anderen Bereichen zu werden. Einige konkrete Handlungsgebiete können wir dennoch nennen.

Industrieunternehmen können durch den Einsatz von „Predictive Maintenance“ mittels Analyse von Sensordaten der Maschinen den Verschleiß und Reparaturbedarf vor einem Ausfall erkennen – und somit Verzögerungen im Produktionsablauf zu vermeiden. Mit Hilfe von „Digital Twins“ (einem virtuellen Abbild der Produktionsanlagen oder Produkte) werden Maschinen und Produkte virtuell erfasst und mit Sensorinformationen verknüpft. Die im Laufe der Zeit gewonnenen Informationen können direkt in die Produktherstellung weitergegeben werden, um die Qualität sukzessive zu verbessern. Wir sehen hier in der Zusammenarbeit mit unseren Partnern und Kunden sehr gute Beispiele für den Einsatz der genannten Lösungen.

Ein weiteres Beispiel ist die Erstellung von Kundenapplikationen, die zusätzlich zu dem eigentlichen Produkt dem Kunden zusätzliche Informationen als Service geben. Solche digitalen Produkte erweitern vermehrt das bestehende Portfolio. Ist einmal die Basis geschaffen, werden hier in immer schnelleren Lebenszyklen neue digitale Produkte im Umlauf kommen.

Neben den bisher genannten eher evolutionären Lösungen können wir auch komplett disruptive Lösungen nennen, wie z.B. die plattformbasierte Lösung DriveNow (<https://www.drive-now.com/de/>). Durch diese Plattform bietet BMW in Kooperation mit Sixt Kurzzeitmieten für BMW Fahrzeuge in Großstädten an. Ein komplett neues Geschäftsmodell, dass mit dem Kerngeschäft der Fahrzeug-



Donald Wachs,
globaler Leiter
Manufacturing bei
BearingPoint und
Experte für Industry
4.0 / IoT

herstellung nicht mehr viel zu tun hat. Lösungen wie unser Infonova R6 (<https://www.infonova.com/de/infonova-r6.html>) helfen Kunden dabei, den End-to-End Concept-to-Cash Prozess zu unterstützen.

Die Potentiale der Evolutionsstufe Get Optimized können nur durch die Optimierung der vorausgehenden Evolutionsstufen in allen Bereichen aufgedeckt werden. Erst durch das Zusammenspiel der verschiedenen Elemente wird eine optimale Implementierung der IoT Technologien erzielt.

Fazit

„Ist IoT ein realer Hype oder eine neue Blase?“ Die Ursprungsfrage können wir mit der Aussage „IoT ist Realität!“ beantworten. Die technologischen Fortschritte der letzten Jahre, die aktuellen Anwendungsfälle, aber auch die anstehenden Lösungen sind zu weit fortgeschritten, um noch umkehrbar zu sein.

Industrieunternehmen müssen sich heute schon auf die 4. industrielle Revolution vorbereiten.

Die Anforderungen an Industrieunternehmen unterscheiden sich dabei nicht so sehr von den Anforderungen an Beratungshäuser, die IoT Projekte bereits seit einiger Zeit durchführen. Wer im Markt bestehen will, muss jetzt schon beginnen die notwendige Kompetenz und Expertise aufzubauen, um schnell genug agieren zu können. Die hohen Anforderungen der IoT-Projekte erfordern eine Bündelung verschiedener Expertisen aus unterschiedlichen Bereichen – Prozesskompetenz, Automatisierungs-, PLM- und ERP-Know-how sind genauso gefordert wie Datenarchitektur und Data Science Wissen sowie ein hohes Maß an IT-Umsetzungskompetenz.

Donald Wachs, Yilmaz Tüfekci

Internet of Things – Game Changer oder Gadget?

Internet of Things (IoT) ist neben der Blockchain Technologie und Voice Assistants eines der Digitalthemen, die derzeit am intensivsten diskutiert werden. Die Meinungen reichen von Euphorie über die neuen Vernetzungsmöglichkeiten bis hin zur Skepsis hinsichtlich des tatsächlichen Mehrwerts für die Anwender.

So kontrovers diskutiert, in einem sind sich die Experten einig: Die Bedeutung von Internet of Things – verstanden als Netzwerk von physischen Geräten (den „Dingen“), die mit Elektronik, Sensoren und Software ausgestattet sind, miteinander bzw. mit den Anwendern verbunden sind und Daten austauschen, – wird künftig zunehmen. So wird erwartet, dass 2020, also schon in zwei Jahren weltweit etwa 25 bis 30 Milliarden verbundene Objekte im Einsatz sind – wobei eine zuverlässige Prognose wohl sehr schwierig sein wird. Die Dimensionen zeigen, wie relevant das Thema in Zukunft sein

wird. Das gilt auch für Konsumgüterhersteller wie Henkel.

Auch wenn einem beim Thema IoT zunächst Konsumenten Anwendungen wie Fitnesstracker, smarte Lautsprecher oder Connected Home-Systeme in den Sinn kommen, möchte ich darauf hinweisen, dass der B2B-Bereich bereits sehr weit entwickelt ist. IoT-Lösungen kommen in der Produktion bei vernetzten Industry 4.0-Systemen zum Einsatz, in den Bereichen Digital Health, Smart Cities oder bei digitalen Retail- und Point of Sale-Lösungen. Dabei mögen die B2B IoT-Anwendungen im Vergleich zu den B2C IoT-Produkten zunächst weniger spektakulär anmuten, sie sind jedoch nicht minder hochentwickelt und relevant, liegen ihnen doch meist konkrete Problemstellungen, Prozesse und Geschäftsmodelle zugrunde.

Ein Rundgang über die CES, die Consumer Electronics Show, auf der im Januar in Las Vegas die neuesten Technik-Innovationen vorgestellt worden sind, zeigt, dass es kaum eine Branche gibt, die heute nicht digital vernetzt ist: Selbstfahrende Autos, sprachgesteuerte Unterhaltungselektronik, intelligente Fitnessgeräte, smarte Küchen oder digitale Haussicherungssysteme sind nur einige der prominenteren Beispiele.

Das Internet der Dinge macht auch vor schlafoptimierenden Betten und schnarch-reduzierenden Kopfkissen, bewegungsprogrammierbaren und videoüberwachten Babywiegen, smarten Eierkochen, Hemdenfaltmaschinen, Katzen-Geotrackern, Mülleimern mit Scanner, die beim Entsorgen der leeren Packungen das entsprechende Produkt direkt nachbestellen, und kindlich anmutenden Robotern, die Hilfe in allen Lebenslagen versprechen, nicht Halt. Jeder der zehntausenden Neuheiten auf der CES liegt sicherlich – bzw. hoffentlich – ein konkreter Anwendungsfall, eine Zielgruppe und auch ein Business Case zugrunde. Dennoch darf bei mancher Innovation die Frage erlaubt sein: Ist das nun wirklich ein Game Changer oder eher ein Gadget? Daher seien hier vier Kriterien genannt, von denen mindesten eins, besser jedoch mehrere erfüllt sein sollten:

- 1.) Produktivitätssteigerung:** Gerade IoT-Anwendungen im B2B-Bereich können helfen, Produktionsprozesse oder Dienstleistungen effizienter zu gestalten, indem beispielsweise Mitarbeiter in der Produktion mit mobilen Geräten oder Datenbrillen ausgestattet werden, die dazu beitragen, die Fehlerquote zu reduzieren oder effizienter zu arbeiten.
- 2.) Kostenreduktion:** IoT-Lösungen können zu nachhaltigen Kostensenkungen beitragen. So können durch Connected Health Systeme mithilfe von digitalen Ferndiagnosen Behandlungs- und Reisekosten optimiert werden und

dem Patienten idealerweise schneller und gezielter geholfen werden.

- 3.) Innovativer, relevanter Kundennutzen, für den eine Zahlungsbereitschaft besteht:** Dieses Kriterium lässt sich nicht immer eindeutig bewerten, da es auch von den individuellen Nutzensvorstellungen abhängt. Ein Beispiel sind smarte Soundsysteme, die es dem Anwender in Verbindung mit Streamingdiensten erlauben, zuhause unbegrenzt die Wunschklassik ohne die etablierten Tonträger bzw. eine klassische Stereoanlage hören und ggf. per Sprachbefehlen steuern zu können.
- 4.) Neue Umsatzpotenziale („Revenue Streams“):** Hier geht es um die Frage, neben dem Verkaufspreis des IoT-Gerätes weitere Umsatzquellen zu erschließen. Nachgelagerte Geschäftsmöglichkeiten können etwa in innovativen Servicemodellen (Stichwort Subscription Services) oder in der Verwertung und Vermarktung der erhobenen Daten liegen (z.B. können die Messdaten eines Fitnesstrackers für Versicherungen wertvoll sein).

Anwendungsbeispiel IoT Beauty Tech: Der digital vernetzte Friseursalon

Eine im Bereich Internet of Things noch eher junge, aber deutlich an Bedeutung gewinnende Kategorie ist die Beauty Care-Branche. Anbieter von IoT-Innovationen sind dabei unter anderem namhafte globale Kosmetikkonzerne, Elektronik-Hersteller oder Start-ups. Beispiele für Beauty Tech-Angebote sind kleine UV-Sensoren, die den Nutzer vor zu viel schädlicher Sonneneinstrahlung schützen sollen, Haut-Tracker zur regelmäßigen Gesichtsanalyse und Falten-Prävention oder vernetzte Badezimmer-Spiegel mit Display und Augmented Reality-Funktion. Die meisten Beauty Tech-Angebote richten sich an Endverbraucher. Hier besteht die Herausforderung darin, regelmäßige Anwendungsfälle zu finden, die sich in die Beauty-Routinen der Konsumenten einfügen.

Wir bei Henkel Beauty Care, einem der weltweit führenden Hersteller von Kosmetikprodukten sowohl im Endkonsumentenbereich (Marken wie Schwarzkopf Taft, Schauma, Gliss Kur, Brillance, Syoss, Fa) als auch im Friseurbereich (u.a. Schwarzkopf Professional, Indola, Kenra), sehen IoT als Chance für neue Geschäftsmodelle und Angebote für unsere Kunden. Als erstes IoT-Projekt haben wir den digital vernetzten Friseursalon entwickelt, also eine B2B Lösung für Salonbesitzer. Dabei haben wir zunächst in Fokusgruppen und „Ideation Workshops“ mit Frisuren aus unterschiedlichen Ländern die „Consumer Journey“ eines Friseurkunden analysiert. Wir wollten verstehen, wie der Friseur seine

Kunden noch besser und individueller beraten und exakt auf sie zugeschnittene Services anbieten kann. Dabei stellte sich heraus, dass geschulte Friseure die äußere Haarqualität bereits sehr gut beurteilen, jedoch die innere Haarqualität, also die Robustheit und den Feuchtigkeitsgehalt der Haare, nicht bestimmen können. Auch ist die Ermittlung der Ausgangshaarfarbe oft subjektiv und durch die Lichtverhältnisse im Salon beeinflusst. Für Friseure ist es jedoch sehr wichtig, die innere Haarqualität und die tatsächliche Haarfarbe zu kennen. Nur so können sie letztlich das geeignete Haarpflegeprogramm oder die passende Haarcoloration auswählen. Aus diesen Anforderungen hat ein bereichsübergreifendes Henkel-Team mit Mitarbeitern des Friseurgeschäfts, des Digitalbereichs sowie der Forschung & Entwicklung das erste digital vernetzte Ökosystem für Friseursalons entwickelt: den Schwarzkopf Professional SalonLab, der erstmals auf der CES im Januar 2018 der Öffentlichkeit vorgestellt wurde. Und das sehr erfolgreich – die Neuheit wurde mit zwei CES Innovation Awards ausgezeichnet.

Das Schwarzkopf SalonLab System besteht aus zwei miteinander vernetzten Geräten: dem SalonLab Analyzer und dem SalonLab Customizer sowie der SalonLab Consultant App, die über ein iPad gesteuert wird, als verbindendes Element.

Das System wird im Friseursalon in drei Schritten angewendet:

Schritt 1: SalonLab Analyzer

Der Schwarzkopf Professional SalonLab Analyzer ist ein Handscanner, der mit Nahinfrarot und Lichtsensoren ausgestattet ist. Er misst die innere Lichtsensoren des Haares, den Feuchtigkeitsgehalt und die exakte Farbe. Um eine repräsentative Haar-Diagnose zu erhalten, wendet der Friseur den Analyzer an verschiedenen Stellen an, von der Wurzel bis zu den Haarspitzen. Anschließend werden die Ergebnisse analysiert und mithilfe eines Algorithmus verarbeitet, dem ein digitalisiertes Haarmodell zugrunde liegt. Kombiniert mit der Expertise des Friseurs ermöglichen die Daten aus der Haaranalyse eine ideale individuelle daten-basierte Beratung.

Schritt 2: SalonLab Consultant App

Die SalonLab Consultant App ist das verbindende Element zwischen den digitalen Geräten. Es handelt sich um eine iPad-App, die den Friseur bei der Haaranalyse unterstützt, die Ergebnisse der Messungen grafisch aufbereitet und eine persönliche Farbberatung mithilfe der Augmented Reality-Technologie ermöglicht. So kann der Kunde im Livebild sehen, wie eine bestimmte Coloration auf seiner individuellen Haargrundlage aussehen würde, bevor sie angewendet wird.



Dr. Nils Daecke, Head of Digital Marketing Beauty Care, Henkel AG & Co. KGaA

Schritt 3: SalonLab Customizer

Der SalonLab Customizer ist eine Mischmaschine für Haarshampoos – direkt im Salon. Er mischt ein personalisiertes Shampoo, das individuell auf die gemessenen Haareigenschaften des Kunden abgestimmt ist. Auf Basis von verschiedenen Pflegestoffen und Parfums können 128 verschiedene Shampoo-Kombinationen gemischt und direkt im Friseursalon abgefüllt werden. Dazu druckt der Customizer ein personalisiertes Etikett aus, das einfache Nachbestellungen ermöglicht.

Dieses IoT-System eröffnet dem Friseur nicht nur neue und exakte Erkenntnisse über die Haarbeschaffenheit seiner Kunden, sondern auch neue Umsatzpotenziale durch Salon-Services wie Haaranalysen, personalisierte Beratungen und individualisierte Produkte. Gleichzeitig wird dadurch für Henkel Beauty Care der Grundstein für disruptive, datengetriebene Geschäftsmodelle gelegt. Denn die im SalonLab gewonnenen Haar- und Anwendungsdaten können wir wiederum, unter Berücksichtigung der neuesten Datenschutz Richtlinien, für die Entwicklung neuer Produkte und Services nutzen.

Game Changer oder Gadget – diese Frage lässt sich bei den meisten IoT-Innovationen erst rückblickend abschließend beantworten. Wir bei Henkel und auch unsere Schwarzkopf Professional-Friseure, mit denen wir den SalonLab entwickelt haben, glauben fest an das Potenzial und den Kundennutzen dieses neuartigen IoT-Systems. Ich bin mir sicher, dass es neue Impulse in der Friseurbranche setzen wird.

Dr. Nils Daecke

Sind deutsche Unternehmen bereit für IoT?

Das Internet der Dinge (IoT) wird sowohl für Unternehmen, als auch für Verbraucher in den kommenden Jahren einen immer höheren Stellenwert erreichen, daran gibt es keinen Zweifel. Bisher sehen sich Unternehmen allerdings mit vielfältigen Herausforderungen konfrontiert, wollen sie IoT-Projekte testen oder umsetzen. Konkret lassen sich aktuell fünf Kernaspekte herausstellen, die die Massenmarkttauglichkeit des Internets der Dinge einschränken:

1. Die Entwicklung von IoT-Projekten ist sehr komplex.

Der Einstieg ins Internet der Dinge erfordert viel Zeit, Geduld und vor allem das entsprechende Budget. Denn IoT-Implementierungen erreichen ihre Rentabilitätsschwelle für gewöhnlich erst nach einigen Jahren der Anwendung, da die kritische Masse an Nutzern erst generiert werden muss. Dies schreckt Unternehmen und Investoren ab.

2. Der Fokus auf den Business Case geht verloren.

Zu oft ist Unternehmen nicht klar, wie sie das Internet der Dinge skalierbar monetarisieren sollen. Durch die aufwendige Suche nach der passenden technischen IoT-Lösung geht häufig der Fokus auf den eigentlichen Business Case verloren.

3. Mangelndes Vertrauen in die Technik.

Sicherheitsbedenken der Verbraucher behindern die Verbreitung des IoT im Endkonsumenten-Markt. Inzwischen hat sich die Annahme festgesetzt, dass eine größere Vernetzung gleichbedeutend mit einem höheren Risiko für die Datensicherheit ist. Es fehlt das Vertrauen in die Sicherheit der technischen Realisierung.

4. Fehlender Mut zur agilen Umsetzung.

Insbesondere große Konzerne neigen dazu, von Beginn an eine „große“ technische IoT-Lösung anzustreben und nur große IoT-Projekte umsetzen zu wollen. Diese Herangehensweise beinhaltet durch ihre Komplexität ein großes Projektrisiko und erfordert eine hohe Startinvestition. Häufig fehlt der Mut, sich dem Internet der Dinge über eine agile Projektumsetzung oder über kleinere Testprojekte anzunähern.

5. Produkte und Services arbeiten nicht eng genug zusammen.

Es besteht der Bedarf nach einer IoT-Lösung, die alles mit allem verbinden kann, die es erlaubt, geräte- und herstellerunabhängig miteinander zu arbeiten und Partnerschaften zwischen Unternehmen zu bilden. Laut eco-Verband beklagen aber zwei Drittel aller deutschen Unternehmen eine fehlende Standardisierung von IoT-Lösungen auf dem Markt. Es bedarf einer Lösung, die eine hohe Interoperabilität bietet, also die Fähigkeit, über die Grenzen von Unternehmen und Systemen hinweg zusammenzuarbeiten.

Interoperabilität ist erfolgskritisch für Unternehmen

Die vollständige IoT-Interoperabilität galt bisher als zu schwer zu verwirklichen, da sie als zu riskant und kostspielig von Unternehmen eingestuft wird. Diese Annahme basiert darauf, dass die meisten Geräte und Dienstleistungen nur mit einem hohen Zeit- und Investitionsaufwand miteinander verbunden werden können. Laut einem Bericht des Analystenhauses Gartner werden in den nächsten Jahren 75 Prozent aller IoT-Projekte doppelt so lange in der Umsetzung brauchen, wie ursprünglich geplant – was unter anderem auf die mangelnde Interoperabilität zurückzuführen ist.

Solange diese Projektrisiken aufgrund der hohen Komplexität existieren, werden viele kleinere

Unternehmen, besonders Dienstleister, vor einer Investition in IoT-Projekte zurückschrecken. Zudem ist eine Anwendung vom Internet der Dinge für den Endverbraucher erst dann attraktiv, wenn eine unendliche Vernetzungsfähigkeit von Geräten mit Dienstleistungen möglich wird.

Erlebte Vorteile durch das Internet der Dinge bieten

Die Relevanz für den Endkunden kann am besten an Funktionalität und Innovation eines Produktes gemessen werden. Diese sind nämlich inzwischen ein größerer Faktor für Kaufentscheidungen, als das Markenimage. Interessant werden solche Produktneuerungen, wenn sie an greifbaren Beispielen verdeutlicht werden, die den konkreten Mehrwert einer IoT-Anwendung für den Verbraucher aufzeigen. So kann etwa ein vernetzter Autoreifen dem Fahrer jederzeit Rückmeldungen über den allgemeinen Zustand und den Luftdruck des Reifens geben und bei entsprechendem Verschleiß direkt nach einem passenden Angebot eines Autohauses suchen. Oder der Fitness-Tracker, der neben einer Aufzeichnung der Aktivität auch die Abnutzung der Sportschuhe berechnet und ab einem gewissen Laufpensum ein Angebot des Sportwarengeschäfts generiert.

Die drei Phasen des IoT im Endkundenbereich

Der Entwicklungsverlauf im Endkonsumentenbereich verdeutlicht am besten, wie umfassend die Interoperabilität vorangeschritten ist. Diese ist für den Erfolg eines IoT-Projekts enorm wichtig. Der Verlauf lässt sich in drei Phasen aufteilen:

Innerhalb der ersten Phase verbinden Unternehmen Geräte mit einem ganz speziellen Anwendungsfall. So kann beispielsweise eine Sicherheitskamera über die Cloud mit dem Smartphone verbunden werden, sodass der Hausbesitzer auch im Urlaub nach dem Rechten sehen kann. Eine solche Verbindung ist typisch für die erste Phase des IoT. Entsprechende Geräte werden mit einer App verbunden, über die sich verschiedene Funktionen steuern lassen. Diese Art der Anwendung hat zwar einen Nutzen für den Endverbraucher, schöpft das vielfältige Potenzial des Internets der Dinge allerdings nicht aus.

In Phase zwei versuchen Unternehmen die in Phase eins beschriebenen Insellösungen untereinander zu vernetzen, wodurch die Konnektivität zu Dritten möglich wird.

Um einen langfristigen Nutzen und somit die Generierung von Mehrwert zu ermöglichen, haben Gerätehersteller und Plattformanbieter damit begonnen, ihre Datenschichten zu öffnen und somit Konnektivität zu Drittanbietern zu ermöglichen.



Axel Godoy, CEO, mozaik

Thema:

**MACHINE LEARNING –
IMPULSE DURCH QUANTEN COMPUTING,
DATA MINING UND REINFORCEMENT LEARNING**

Heute lernen, die Zukunft zu gestalten.

DIGICON 2018**DIGITALE WELT CONVENTION****AUSZUG UNSERER HOCHKARÄTIGEN REFERENTEN**Prof. Dr. Claudia Linnhoff-Popien
LMU München
Digitale Stadt München e. V.Prof. Dr. Fredmund Malik
CEO & Erfolgsautor
Malik Institute for Complexity and ManagementProf. Dr. Katharina Morik
Lehrstuhl für künstliche Intelligenz
TU DortmundDr. Jörg Ochs
Geschäftsführer
SWM Infrastruktur
Verwaltung GmbHThomas Schlereth
Geschäftsführer
Can Do GmbHDr. Roland Schütz
EVP and CIO
Lufthansa Group Airlines
and Digital InitiativesProf. Dr. Patrick van der Smagt
Director AI Research
VW GroupDr. Heiko Udluft
Data Scientist & Tech-Team Lead
AirbusDr. Johannes Wechsler
CIO
ProSiebenSat.1 Media SE**21. UND 22.
NOVEMBER 2018**
Palais Lenbach, MünchenFür Ihre Anmeldung sowie weitere Informationen gehen Sie bitte auf unsere Webseite www.digitaleweltmagazin.de/digicon



Felix Heimbrecht,
Director Technology
for Emerging Experiences,
Publicis Sapient EMEA APAC

Die dritte Phase des IoT nutzt erstmalig das volle Potenzial des IoT aus, indem es alles miteinander vernetzt, was vernetzt werden kann. Dafür ist eine universelle Interoperabilität unerlässlich. Durch eine so gewährleistete Kommunikationsfähigkeit der Geräte mit Dienstleistern werden alle denkbaren datengetriebenen Anwendungsszenarien möglich und somit eine große Relevanz für den Endkonsumenten geschaffen.

IoT-Lösung muss Datenschutz und IT-Sicherheit beachten

Eine solch vielfältige und weitverzweigte Vernetzung weckt allerdings auch Ängste: Unter den Endkonsumenten herrschen noch große Sicherheitsbedenken, wenn es um den Datenschutz im IoT-Umfeld geht. Diesem Misstrauen müssen Unternehmen vorbeugend mit technischen Lösungen begegnen. Den Endkonsumenten sollte innerhalb eines Systems stets selbst die Möglichkeit gegeben werden, mit wem welche Daten geteilt werden. Eine solche Transparenz wirkt sich positiv auf das Vertrauen der Verbraucher aus. Eine IoT-Lösung sollte nach dem Security-by-Design-Prinzip entworfen werden. Die im Mai 2018 in Kraft tretende EU-Datenschutzgrundverordnung muss dabei stets im Auge behalten werden.

Hürden sehen und überwinden

Der IoT-Markt wird in den kommenden Jahren stetig weiterwachsen. Damit Unternehmen und Verbraucher hieraus den größtmöglichen Mehrwert ziehen können, müssen die Anwendungsszenarien für den Endkonsumenten relevant und attraktiv sein. Um dies zu erreichen, ist eine allumfassende Verbindung von Geräten mit Services Voraussetzung. Diese Vernetzung sollte wiederum über eine IoT-Plattform erfolgen, die dabei wie ein Marktplatz aufgebaut ist. Über diesen können alle Anbieter und Anwender zusammenkommen, um Devices und Services zu handeln.

Axel Godoy

IoT und AI: eine Co-Evolution

Das Internet der Dinge und künstliche Intelligenz gehören zu den beherrschenden Innovationstrends der letzten Jahre. Beide haben aufgrund der schnellen technologischen Entwicklung einen gewissen Reifegrad erreicht und zu ersten praktischen Anwendungen geführt, kämpfen aber nach wie vor mit diversen Herausforderungen und Unzulänglichkeiten. Obwohl beide Trends in aller Ausführlichkeit diskutiert werden, wird der enge Zusammenhang dieser Technologien seltener betrachtet. Dabei könnten gerade die Wechselwirkungen für ihren Erfolg entscheidend sein.

Internet of Things: Der mühsame Weg von der Vision zur Realität

Die Kernidee hinter dem Internet der Dinge ist, dass sehr kleine und miteinander vernetzte Computer zu Bestandteilen von Gegenständen und der Umgebung werden. Damit wird letztlich der Computer als Gerät verschwinden.

Umgekehrt könnte man auch sagen, dass Computer als integrale Komponenten in der menschlichen Umwelt allgegenwärtig werden (Ubiquitous Computing). Diese aus den 90er Jahren stammende Vision wird zunehmend real. Die steigende Rechenleistung ist einer der Treiber dieser Entwicklung. Auch die verbesserte Energieeffizienz und die allgegenwärtige Konnektivität tragen dazu bei. Schließlich verfügen wir heute über eine neue Generation von hochintegrierten und multimodalen Sensoren, Big-Data-Systemen sowie leistungsfähiger Cloud-Dienste.

Es gibt aber noch viele Probleme zu lösen. Sicherheitsprobleme, fehlende Standards oder mangelnde Kompatibilität durch proprietäre Protokolle gehören dazu. Zudem wird der beschränkte Gesamtnutzen der momentan meist noch inselartigen Lösungen kritisch betrachtet. So spricht mancher aktuell gar vom „Internet of Shitty Things“.

Ein wirklich funktionierendes und sinnhaftes Netz der Dinge ist enorm komplex: Es besteht nicht nur aus vielen unterschiedlichen Komponenten, sondern ist vor allem auch dezentral organisiert. Zudem erfordert es vielfältige neue Formen der Interaktion mit Menschen.

Herkömmliche Nutzerinterfaces – wie Touchscreens – sind häufig kein gangbarer Weg mehr. Dies liegt zum einen schlicht am benötigten Platz und dem vergleichsweise hohen Stromverbrauch solcher Komponenten. Zum anderen sind natürlichere Interaktionsformen das erklärte Ziel. Dafür müssen IoT-Lösungen intelligent agieren, unter anderem in dem sie Kontext verstehen. Diese Erwartung äußert sich auch darin, dass das Wort „Smart“ in praktisch allen Anwendungsfällen von IoT auftaucht: Man spricht auf Netzebene beispielsweise von Smart Grids, Smart Cities, Smart Mobility, Smart Home oder Smart Manufacturing und auf Geräteebene von Smart Speakern, Smart Wearables und Smart Phones.

Artificial Intelligence: Der erste Sommer

Der aktuelle Hype ist nicht der erste in der mittlerweile fast siebzigjährigen Geschichte der künstlichen Intelligenz. In der Vergangenheit gab es immer wieder kurzfristige Erfolge in Laborsituationen, die zunächst für Durchbrüche gehalten wurden, sich dann aber in der praktischen Anwendung als herbe Enttäuschung erwiesen. Dies hat anschließend immer wieder zur weitgehenden Einstellung der Forschungsaktivitäten geführt

– den sogenannten AI-Wintern. Die Situation ist diesmal anders: Der massive Fortschritt der sogenannten neuronalen Netzwerke hat zum ersten Mal in der Breite zu praktisch anwendbaren Lösungen geführt. Insbesondere in der Bilderkennung (Computer Vision), der Sprachverarbeitung (Speech Recognition) und dem Textverstehen (Natural Language Understanding) sind diese Technologien sogar bereits in den Wohnzimmern angekommen – beispielsweise in Form von Smart Speakern. So kann heute jedermann mit dem Amazon Echo Look nicht nur sprechen. Dieser kann sein Gegenüber sogar sehen und daher auf Basis des aktuellen Outfits Modetipps geben.

Diese Technologie ist universell einsetzbar und wird unter anderem erfolgreich zum Data Mining, zum Erlernen von Spielen (z.B. Googles AlphaGo) und zum Verbessern oder Erzeugen von Bildern genutzt. Es geht hierbei aber nicht um künstliche „Intelligenz“ im eigentlichen Sinne, sondern um einen kleinen Teilbereich der AI – nämlich um maschinelles Lernen (ML).

Neue Architekturen für neuronale Netzwerke, sogenannte Deep Neural Networks (DNNs), verbunden mit der mittlerweile zur Verfügung stehenden Rechenleistung und der Speicherkapazität, haben zu einem Paradigmenwechsel geführt: Hartnäckige, komplexe und hochdimensionale Probleme, die die Informatik trotz jahrzehntelanger Anstrengungen bisher algorithmisch nicht zufriedenstellend in den Griff bekam (z.B. Spracherkennung), können jetzt plötzlich gelöst werden. Und zwar indem ein System mit Beispielen trainiert wird und so selbstständig Zusammenhänge erlernt. Daraus resultierend kann dieses System anschließend auch für unbekannte Eingaben die richtigen Ergebnisse liefern. Aber genau in diesem Training steckt auch eine der Herausforderungen der neuen Technologien – sie benötigen Unmengen an qualitativ hochwertigen Trainingsdaten.

AI braucht IoT

Eine der zentralen Voraussetzungen für Machine Learning ist also die Verfügbarkeit von digitalen Daten. Nicht umsonst gehört beispielsweise die Bilderkennung zu den ersten erfolgreichen Anwendungsgebieten: Es gibt mittlerweile unzählige kategorisierte oder mit Text annotierte, digitale Bilder – z.B. aus den sozialen Netzwerken oder Suchmaschinen. Ebenfalls gehören Übersetzungen zu den Vorreitern des Machine Learning. Digital vorliegende Texte, wie etwa die Dokumente der Europäischen Union mit ihren 23 Amtssprachen, können als Trainingsdaten genutzt werden.

Der erfolgreiche Einsatz von KI in anderen Bereichen wie dem autonomen Fahren hängt ebenfalls von der verfügbaren Datenmenge ab – zum einen

für das Training der Modelle, zum anderen aber auch für die Steuerung des Fahrzeugs in Echtzeit. Dafür werden unterschiedlichste Sensoren benötigt, die solche Daten in benötigter Menge, Geschwindigkeit, Qualität und Auflösung liefern können. IoT-Netzwerke gehören damit zu den wichtigsten Enabler für den Einsatz von künstlicher Intelligenz im physikalischen Raum.

IoT braucht AI

Auch ein funktionierendes Internet der Dinge ist ohne einen gewissen Grad an „künstlicher Intelligenz“ schwer vorstellbar oder würde letztlich nur enttäuschend einfache und starre – weil programmierte – Anwendungsfälle ermöglichen. Doch große Datenmengen zu verarbeiten, darin Zusammenhänge und Muster zu erkennen und komplexe Steuerungen zu realisieren, sind die Paradisdisziplinen von Machine Learning. Um IoT intelligenter zu machen, können diese Funktionalitäten auf verschiedenen Ebenen des Systems zur Anwendung kommen:

1. Verarbeitung von Sensordaten

Moderne, hochintegrierte Mehrfachsensoren sowie Kameras und Mikrofone liefern viele Rohdaten, aus denen idealerweise schon im entsprechenden IoT-Gerät die entscheidenden Informationen gefiltert oder vorverarbeitet werden können (z.B. Entfernungssensoren, die bereits Messfehler glätten oder Überwachungskameras, die nicht mehr ein Bild, sondern strukturierte Daten über erkannte Objekte liefern). Das macht nicht nur die Nutzung von schmalbandigen Verbindungen effizienter, sondern verhindert auch Latenzen – also Verzögerungen, die entstehen, wenn große Datenmengen an eine zentrale Instanz übertragen werden müssen. Diese Instanzen müssen diese Daten dann noch verarbeiten, Entscheidungen treffen und Steuerungsbefehle in die umgekehrte Richtung geben – das addiert sich schnell zu Zeiten, die aufgrund des Echtzeitcharakters vieler IoT-Systemen problematisch sind. Je intelligenter die Komponenten eines Netzwerkes sind, desto robuster und schneller kann es funktionieren und desto mehr Anwendungsmöglichkeiten gibt es.

2. Steuerung des Gesamtsystems

Da ein wesentlicher Mehrwert von IoT in der Zusammenarbeit seiner Komponenten besteht, müssen Daten zusammengeführt und darin Muster und Zusammenhänge erkannt werden. Die einzelnen Komponenten liefern nur Informationen über einen kleinen Teilaspekt der Welt. Deshalb ist ein Kontext zu bilden, in dem eingehende Informationen interpretiert und basierend darauf Aktionen ausgelöst werden können.

3. Neue Benutzerschnittstellen

Da Rechner miniaturisiert und etwa in Alltagsgegenständen integriert werden, sind – wie bereits erwähnt – herkömmliche Nutzerinterfaces keine adäquaten Lösungen mehr. Stattdessen tritt die unmittelbare Interaktion des Nutzers mit dem Gerät in den Vordergrund, beispielsweise durch Annäherung, Positions- oder Lageänderung, Gestik oder Mimik oder auch durch sprachbasierte Interfaces. Gerade letztere haben großes Potenzial, weil sie universell sind und über Dialoge komplexe aber natürliche Interaktion ermöglichen – sogar über eine gewisse Distanz. Zudem sind Conversational Interfaces auch relativ einfach in kleineren Geräten integrierbar.

Das Internet der Dinge wird nur erfolgreich sein, wenn grundlegende Probleme wie Interoperabilität und Sicherheit gelöst werden. Vor allem aber muss es letztlich tatsächlich „smart“ sein. Die aktuellen Entwicklungen der AI liefern dafür neue Möglichkeiten und Werkzeuge. Insbesondere, weil Machine Learning optimal geeignet ist, um Zusammenhänge und Muster in großen Datenmengen zu erkennen und bereits ausgereifte Technologien für IoT-kompatible Benutzerschnittstellen zur Verfügung stellen. Umgekehrt steht AI vor dem entscheidenden Sprung von der rein virtuellen zur realen, physikalischen Nutzung, die erst durch IoT-Systeme möglich gemacht wird. Diese Co-Evolution beider Technologien wird sehr wahrscheinlich zu einer Beschleunigung der Entwicklung in beiden Bereichen führen.

Felix Heimbrecht

1.1.2 Strategien

„Industrial Internet of Things“-Lösungen helfen uns allen – wenn die Anbieter ihre Hausaufgaben machen

In einem früheren Beitrag in diesem Blog wurde die Frage gestellt, ob deutsche Unternehmen bereit für das Internet of Things sind. Dass das Internet der Dinge an Bedeutung gewinnt, im privaten wie im industriellen Umfeld, bleibt unbestritten. Man kann quasi dabei zuschauen, wie sämtliche Lebensbereiche von IoT-Geräten und -Lösungen durchzogen werden.

Wer seine Wohnung mit heute noch ausschließlich mit einem metallenen Schlüssel aufsperrt, dem seien die Worte des Zukunftsauteurs William Gibson ans Herz gelegt: „The future is already here — it's just not very evenly distributed.“, die Zukunft ist schon da, nur eben nicht überall gleichmäßig verteilt. Eine Vielzahl neuer Gebäude wird beim Bau mit elektronischen Zugangskontrollen ausgestattet, die per Fingerabdruck oder Handy-App Einlass gewähren. Einige davon sind per WLAN mit ent-

sprechenden Gegenständen im Inneren des Hauses verbunden.

Die vergangenen Jahre haben, gerade was IoT im Consumer-Bereich angeht, gezeigt, dass viele Anbieter noch nicht verstanden haben, was IoT mit sich bringen muss, und was für das Industrial Internet of Things unerlässlich ist.

1. After-market-support

Sobald es um vernetzte Geräte mit eingebetteter Software geht, beschränkt sich der Lebenszyklus eines Produktes nicht länger auf das Verkaufen und die Versorgung mit anfassbaren Ersatzteilen. Die Software-Stacks von IoT-Produkten sind kompliziert genug, so dass es keine Frage ist, ob Sicherheitslücken gefunden werden, sondern lediglich wann. Das leicht angreifbare Sexspielzeug bringt einen noch zum Schmunzeln, aber für ähnlich unsichere Systeme in einem Fertigungsumfeld oder in einer kritischen Infrastruktur hätten die Betreiber sicher weniger Humor übrig.

2. Klare, verlässliche Produktlebenszyklen und Kommunikation

Als Besitzer eines Smartphones kennt man die leidige Frage: „Bekomme ich noch Updates? Bis wann?“ Tatsächlich findet man nur einen einzigen Hersteller in den Weiten des Internets, der am Tag der Vorstellung eines neuen Smartphone-Modells auf der zugehörigen Website den Software-Update-Lebenszyklus veröffentlicht. Im consumer-IoT ist es leider immer noch völlig normal, dass der Käufer dem Prinzip Hoffnung ausgeliefert ist. Für Industriebetriebe, wo die Investition in die kommenden vernetzten Geräte einen spürbaren Anteil an den Geschäftsfinanzen darstellt, ist das inakzeptabel und ein Grund, zu dem Hersteller zu wechseln, der es besser macht.

3. Geplante Obsoleszenz

Obwohl sich die größten Smartphone-Hersteller gerade Sammelklagen wegen geplanter Obsoleszenz einfangen, ist wohl kaum davon auszugehen, dass das nächste iPhone oder das nächste Galaxy S als Flop enden wird. Solange die Geräte Schmuckstücke sind, die zur Mode des jeweiligen Jahres gehören, bestrafen Endkunden die Hersteller nicht für Versäumnisse. Im industriellen Umfeld, das weniger emotional und mehr ökonomischen Faktoren dominiert ist, sollten Hersteller die Finger von fragwürdigen Obsoleszenzpraktiken lassen. Ansonsten werden die Kunden durchaus kreativ, wie im Falle von John Deere. Um die kostspieligen Maschinen des Landmaschinenherstellers länger als vom Hersteller erwünscht reparierbar zu halten, arbeiten dann die Farmer schon mal mit der Hacker-Gemeinde zusammen und sorgen dafür, dass

der Traktor nicht ersetzt werden muss, sondern von einer örtlichen Werkstatt repariert werden kann.

Das alles wird im Industrial IoT noch wichtiger, denn da liegen die Dinge noch komplexer als bei Endkundenprodukten. Während sich für den Endkunden beispielsweise ein Kühlschrank als ein einzelnes „Thing“ darstellt, handelt es sich aus Herstellersicht schon um ein verteiltes System von mehreren gegebenenfalls vernetzten Teilen, wie Kompressor, Temperatursensoren, Luftfeuchtesensoren, bis hin zu Kameras, die den Inhalt des Kühlschranks nachverfolgen und den Besitzer via App erinnern, dass es langsam an der Zeit ist, einzukaufen. Umso komplexer sind dann Produktionsmaschinen und Anlagen, die aus einer Vielzahl von Modulen und Aggregaten bestehen – oft von unterschiedlichsten Herstellern. Eine umfassende Standardisierung ist deshalb unverzichtbar, und zwar auf allen Ebenen der IIoT-Architektur.

Sobald es an Themen wie Produktionsprozesse geht und Menschen im System mitspielen, kommen zusätzliche Herausforderungen wie Echtzeitfähigkeit und funktionale Sicherheit dazu, was im consumer-IoT großflächig ausgeklammert ist. Das wiederum bedeutet empfindliche Einschränkungen für die Software-Architektur solcher Systeme. Ein Modell „Wir laden mal alle Daten in die Cloud und schauen dann.“ funktioniert dann nämlich nicht mehr: die benötigten Antwortzeiten können nicht immer eingehalten werden, und das System ist vor allem nicht garantiert ausfallsicher. Folglich sind die Infrastrukturen, die wir aufbauen müssen, komplexer als die im Endkundenumfeld. Oder es braucht intelligente Lösungen, um die Daten möglichst nah an den Feldgeräten zu verdichten und zu verarbeiten.

Auch bei der Cybersecurity müssen im industriellen Umfeld andere Maßstäbe angelegt werden, die sich eher an den Maßnahmen für kritische Infrastrukturen orientieren müssen als an vielen Consumer-Geräten. Hacker-Angriffe, die das heimische WLAN oder die privaten IoT-Geräte lahmlegen oder kapern, können in der Industrie für immensen wirtschaftlichen Schaden sorgen. Siemens hat deshalb mit renommierten Partnern eine Charter of Trust ins Leben gerufen, die einen neuen Rahmen für Cybersecurity in der Industrie absteckt.

Die Neuerungen und Verbesserungen, die das Industrial Internet of Things verspricht, wie effizientere, kostengünstigere, individualisierte Produktion, bessere Mensch-Maschine-Kollaboration, Optimierung von Wartungsaufwänden, sind alle erreichbar – und sie bieten die Basis dafür, die Industrie mit digitalen Technologien deutlich voranzubringen. Aber nur, wenn die Anbieter ihre Hausaufgaben machen.

Dr. Thomas Zander, Markus Weinländer

Die drei Ausprägungen des IoT und was wir dafür tun können, dass unsere digitale Zukunft eine gute Zukunft wird

Das Internet of Things gibt es, Stand heute, in drei Ausprägungen: Smart Home, Smart World und Industrial IoT. Die drei Bereiche sind unterschiedlich weit entwickelt und auch die Prognosen decken sich nicht vollständig – daher lohnt sich ein Blick auf die Details. Die entscheidende Frage, die sich danach stellt, ist jedoch immer die gleiche: Was können wir dafür tun, dass das Internet of Things – und damit unsere digitale Zukunft – gut wird?

„Das Tempo des Wandels war noch nie so schnell und wird nie mehr so langsam sein wie heute.“ So hat es Justin Trudeau, der Premierminister Kanadas auf dem World Economic Forum in Davos formuliert. Besser kann man nicht ausdrücken, was die steil ansteigenden, teilweise exponentiell verlaufenden Kurven bedeuten, die für uns Tecchies zum Alltag gehören. Trudeau diktierte der versammelten Elite auch, wie wir mit diesen „enormen Chancen“ und dem „riesigen Potenzial“, wie wir mit den „Verheißungen“ auf ein „besseres Leben, Innovationen, bemerkenswerte Produkte“ umgehen sollten: „Wir müssen diesen Wandel annehmen und vorantreiben. Jeder einzelne von uns.“

Um den Wandel anzunehmen, muss man ihn erst einmal verstehen. Für das IoT hat eco – Verband der Internetwirtschaft e.V. daher gemeinsam mit Arthur D. Little detaillierte Studien und Analysen vorgelegt über die Bereiche Smart Home[1], Smart City[2] und Industrial IoT[3], jeweils für den deutschen Markt. Hier die wichtigsten Fakten:

Smart Home: Die ersten Erfahrungen und die größten Bedenken

Smart Home ist bereits ein umkämpfter Markt. Die Studie erwartet, dass der Markt in den nächsten Jahren jährlich weiter stark wächst, und zwar um knapp 27 Prozent pro Jahr. 2022 kann der Markt für Smart Home-Lösungen in Deutschland bereits 4,3 Milliarden Euro erreichen.

Im Smart Home geht es im wesentlichen um die Frage: Wie können wir effizienter und komfortabler wohnen? Im Kern stehen Herausforderungen wie steigende Energiepreise, mangelnde Zeit für Hausarbeiten, Sicherheit und der Anstieg von Pflegebedürftigen. Viele der damit verbundenen Aufgaben können wir mit einem vernetzten Zuhause effizienter und zuverlässiger lösen.

Das Smart Home ist nicht nur für IT-Unternehmen ein wichtiger Markt, ein wirklich sinnvoll vernetztes Zuhause ist ein Ökosystem, das neben Telekommunikationsdienstleistern auch Versorger, Handwerker und Haushaltsgerätehersteller, Logistiker und Lebensmittellieferanten umfasst. Diese Akteure lassen sich in sechs Segmente einteilen:



Dr. Thomas Zander,
Principal Engineer im
Technologiefeld IoT,
Siemens Corporate
Technology

Energiemanagement, Licht- und Fenstersteuerung, Sicherheit und Zugangskontrolle, Unterhaltung, Haushaltsgeräte sowie Gesundheit und betreutes Wohnen.

Aus Sicht der Bewohner eines Smart Homes ist angesichts dieser Vielfalt klar: Wirklich sinnvoll sind die vielen verschiedenen Lösungen nur dann, wenn sie alle miteinander über eine einzige, zentrale Steuereinheit bedient werden können. Ein Beispiel für ein sogenanntes offenes System ist ein smartes System von Überwachungskameras, welches bei Betreten der Wohnung nicht nur per Gesichtserkennung registriert, wer im Haus ist, und das Abschalten der Alarmanlage auslöst, sondern die Tür automatisch entriegelt, das Entertainment-System aktiviert und die Lichter im Eingangs- und Wohnbereich einschaltet.



Harald A. Summa,
Geschäftsführer,
eco e.V.

Smart City: Nachhaltig und ganzheitlich Leben in der Stadt

Deutsche Städte haben bereits damit begonnen, nachhaltige und ganzheitliche smarte Stadtkonzepte zu entwickeln. Die Studie schätzt, dass der zugehörige Markt pro Jahr um mehr als 16 Prozent zulegt und 2022 43,8 Milliarden Euro erreicht. Die größten Versprechen der Smart City ergeben sich aus den größten Problemen, die das Leben in der Stadt mit sich bringt: Verkehrschaos, zunehmende Verschmutzung und Probleme bei der Altersversorgung, effiziente Versorgung mit essentiellen Gütern wie Energie und Nahrung und natürlich auch das Thema Sicherheit.

Genau wie im Smart Home ist auch die Smart City nur denkbar als Ökosystem. Allerdings ist hier die Vielzahl und Unterschiedlichkeit der Akteure noch größer. Zehn verschiedene Segmente nennt die Studie: Transport und Logistik, Kommunikationsdienste und Netzwerksicherheit, physische Sicherheit, Gebäudeautomatisierung, Gesundheitswesen, Energie, Tourismus und Einzelhandel, Bildung, Finanzdienstleistung sowie öffentliche Verwaltung.

Lösungen im Bereich Smart City sind auf den ersten Blick weniger abhängig von der Akzeptanz von Endkunden, die einzelnen Bewohner stehen dennoch im Vordergrund. Ein Musterbeispiel ist Dubai, eine Stadt, die bereits mehr als 1.000 verschiedene Smart-City-Dienstleistungen aus den unterschiedlichsten Segmenten anbietet und dabei auf ein offenes und segmentübergreifendes Plattformkonzept setzt. Die Verbesserungen spielen sich nicht nur im Hintergrund ab, sondern sind durchaus im Alltag spürbar, beispielweise beim Verkehrsfluss und den CO₂-Emissionen.

Industrial IoT: Vorzeigestandort Deutschland

Die Zahlen im Bereich Industrial IoT sehen auf den ersten Blick gar nicht so viel anders aus bei

Smart Home und Smart City. Die Studie rechnet mit etwa 19 Prozent jährlichem Wachstum und einem Volumen von 16,8 Milliarden Euro im Jahr 2022. Dennoch unterscheidet sich Industrial IoT deutlich von Smart Home und Smart City. Der Standort Deutschland ist hier im internationalen Vergleich deutlich besser positioniert.

Effizienzsteigerung und Automatisierung: Das sind die beiden großen Ziele, die in der Regel mit Industrial IoT-Projekten verwirklicht werden sollen. Wie weit Unternehmen auf diesem Weg fortgeschritten sind, lässt sich besonders gut an einer Kennzahl ablesen: der Roboterdichte.

Die deutsche Industrie profitiert im Bereich Industrial IoT von ihrem Innovationsgeist und ihrem im internationalen Vergleich höheren Automatisierungsgrad. Hier ist Deutschland neben den asiatischen Industrienationen (Südkorea, Japan) führend. Während die Roboterdichte pro Industriebeschäftigten weltweit bei knapp 70 pro 10.000 Beschäftigte liegt, ist Deutschland mit rund 300 Robotern pro 10.000 Beschäftigte unter den Top 5 Nationen weltweit.

Genau wie in den Bereichen Smart Home und Smart City ist auch im Industrial IoT die Vernetzung, also die Ausbildung von Ökosystemen entscheidend. Hier zeigt sich auch, wo noch Potenzial liegt: Denn die meisten derzeit verwendeten Industrial IoT-Lösungen stehen noch weitgehend für sich allein. Ganzheitliche Projekte, welche idealerweise die gesamte Supply Chain umfassen, sind das Ziel, derzeit aber noch die große Ausnahme.

Sieben Segmente benennt die Studie: Automobil, Maschinenbau, Elektro und Elektronik, Metall, anderes verarbeitendes Gewerbe, Versorger sowie Bau-, Land- und Forstwirtschaft.

Was können wir tun, dass unsere digitale Zukunft eine gute Zukunft wird?

Smart Home, Smart City und Industrial IoT: In allen drei Bereichen steckt ein enormes Potenzial und in allen drei Bereichen sind es ähnliche Faktoren, die über den Erfolg entscheiden. Einer der wichtigsten, der vielleicht wichtigste ist die Frage, ob uns die Vernetzung gelingt. Nicht Einzellösungen gehört die Zukunft, sondern Ökosystemen. Offene Schnittstellen, gemeinsame Standards, zentralisierte Bedienung, einheitliche Benutzerführung, Kooperation statt Konkurrenz: Das sind die Faktoren, auf die es im IoT ankommt.

Wir sollten das volle Potenzial nutzen: Nicht nur von IoT – sondern der Digitalisierung insgesamt; nicht nur für die Wirtschaft – sondern für die Gesellschaft insgesamt. Wollen wir das schaffen, müssen wir noch an unserer digitalen Kompetenz arbeiten. Digitale Kompetenz ist nicht ausschließlich technischer Natur. Sie beginnt in unseren

Köpfen und hat viel zu tun mit Eigenschaften wie Zuversicht, Voraussicht und Souveränität. Sie hat zu tun mit dem Willen, sich auf den Wandel einzulassen und die Zukunft zu gestalten.

Im Smart Home, in der Smart City und im Industrial IoT heißt das: Über Grenzen hinweg denken, vor allem die im eigenen Unternehmen. Kompetenzen bündeln. Gemeinsame Standards schaffen, auch und gerade beim Datenschutz und der Transparenz. Auf die Kunden hören und das nicht erst, wenn das Produkt ausgeliefert ist, sondern schon beim Design. Die richtige Balance finden zwischen Kontrolle und Offenheit. Darauf vertrauen, dass alle Beteiligten besser fahren, wenn sie gemeinsam fahren. Kurz: Sich auf das digitale Ökosystem einlassen.

Justin Trudeau hat in seiner Rede auch über die Angst vor dem Wandel gesprochen und die Verantwortung der Politik betont: Für manche Leute sei „Technologie vielleicht ein Vorteil im Privatleben, aber eine Bedrohung für ihren Arbeitsplatz.“ Diese Angst müsse man erst nehmen und viele Politiker müssten noch umdenken. Mehr in zukunfts- und tragfähige Konzepte investieren.

Als Vertreter der Industrie freue ich mich über derartige Einsicht und Entschlossenheit. Was das IoT angeht, kann ich sagen: Hier zeigt sich, dass der Wandel – langfristig und global betrachtet – mehr Sicherheit und Wohlstand bringen kann. Oder wie es Lars Riegel, Principal von Arthur D. Little, formuliert: „Wenn man die globale Perspektive einnimmt, so ist gerade eine Führungsposition im Industrial IoT langfristig ein Garant von Arbeitsplätzen, denn die zunehmende Automatisierung führt zu einer Stärkung der Wettbewerbsfähigkeit deutscher Unternehmen im globalen Umfeld.“

Klingt wie eine große Aufgabe? Ist es auch. Ob uns der digitale Wandel am Ende wirklich gelingt? Ist noch nicht entschieden. Aber immerhin haben wir es selbst in der Hand.

Harald A. Summa

Referenzen: [1] „Der deutsche Smart-Home-Markt 2017-2022. Zahlen und Fakten“ [2] „Der deutsche Smart-City-Markt 2017-2011. Zahlen und Fakten“ [3] „Der deutsche Industrial-IoT-Markt 2017-2022. Zahlen und Fakten“

NarrowBand IoT – der schlanke Einstieg ins Internet der Dinge

NarrowBand IoT (NB-IoT), Low Power Wide Area Network (LPWAN), Edge Computing oder – mit einem Hauch von Poesie – Smart Dust: All das sind Begriffe für eine relativ junge Technologie, die das Internet der Dinge (Internet of Things, IoT) weit nach vorne bringen kann.

NarrowBand IoT definiert einen Funkstandard für Sensoren, Konnektoren und Aktoren, die wartungsfrei und oft unabhängig von externer Stromversorgung in einem langen Leben Daten erheben und zur weiteren Verarbeitung an ein Gateway

übertragen. Diese Befehlskette funktioniert auch andersherum, wenn sie von einem solchen Gateway Befehle erhalten und ausführen. NarrowBand IoT ist damit eine Schlüsseltechnologie der Mobilfunkanbieter für das Internet der Dinge.

Sensor, Konnektor, Aktor: Die Technik hinter der Technologie

Sensoren werden die meisten kennen: Es handelt sich um ein Bauteil, das Eigenschaften der Umwelt wahrnehmen kann, zum Beispiel Schall, Temperatur, Licht, Beschleunigung, Lage oder auch die chemische Zusammensetzung der Umgebung. Konnektoren sind im Grund genommen nichts anderes als Schnittstellen, die von Sensoren aufgenommene „Sinneseindrücke“ oder Messdaten in Netze einspeisen und für die Datenverarbeitung weiterleiten. Aktoren schließlich sind Bauteile, die auf Basis von Befehlen aus Computerprogrammen oder aufgrund von vorliegenden Daten bestimmte Aktionen ausführen. In der einfachsten Form funktioniert die Zusammenarbeit von Sensoren, Konnektoren und Aktoren auch direkt und ohne NB-IoT, zum Beispiel wenn ein Sensor eine bestimmte maximale Wassermenge in einem Kessel registriert, diesen Wert über einen Konnektor weiterleitet und ein Aktor dann ein Ventil schließt, wenn die Wassermenge eine bestimmte Füllhöhe überschreitet.

Hinter der Mobilfunktechnologie NarrowBand IoT agiert eine komplexe Netzwerk- und Dateninfrastruktur aus Datenbanken, Algorithmen und Dashboards, die allesamt dazu dienen, einfache sensorische Daten zu übertragen, zu speichern, zu verarbeiten und damit bestimmte Aktionen und Reaktionen hervorzurufen.

Reicht bis in den tiefsten Keller

Wer bisher über die Voraussetzungen für das Internet der Dinge gesprochen hat, meinte vor allem Breitbandverkabelung, klassische Mobilfunkverbindungen und Cloud Computing. Für einen Teil dieser Anwendungsgebiete, bei der es um die Übertragung großer Datenmengen nahezu in Echtzeit geht, ist das auch weiterhin richtig. Allerdings decken drahtlose und breitbandige Netze längst nicht alle Anwendungsszenarien ab und sind für viele Einsatzzwecke schlicht überdimensioniert.

Hier kommt NarrowBand IoT ins Spiel: Es bietet eine hohe Reichweite bis in entlegene Winkel von Gebäuden hinein („Deep Indoor“). Es unterstützt aufgrund des geringen Energiebedarfs auch einfache Geräte ohne externe Stromversorgung. Es ist wartungsarm und damit auch für Szenarien geeignet, die sich nur dann rechnen, wenn sie preiswert und wenig aufwendig aufzubauen und zu managen sind.

Diesen Vorteilen steht ein Nachteil entgegen: Der Ausbau und Betrieb der NarrowBand IoT-Netze



Christoph Henkels,
Senior Manager und
Unit Leader, Sopra
Steria Consulting

erfolgt aktuell durch die Mobilfunkanbieter, woraus sich eine gewisse Abhängigkeit (das so genannte Vendor Lock-In) ergeben könnte, die sich allerdings nicht einfach vermeiden lässt.

Smart Home & Smart City: Hier sind schlanke Netze genau an der richtigen Stelle

Ein sehr plastisches Beispiel für die Nutzung des noch jungen NarrowBand IoT sind so genannte Smart Meter, also „intelligente Zähler“. Anders als zum Beispiel Stromzähler hängen die Uhren für Gas und Wasser nicht am Stromnetz und sind zudem oft im Keller angebracht, also dort, wo der Mobilfunkempfang nur schwach oder gar nicht möglich ist. NarrowBand-IoT-Sensoren können diese Versorgungslücke schließen und damit das so genannte Smart Home deutlich pushen.

Aber auch außerhalb des eigenen Heims ist NarrowBand IoT sinnvoll, etwa bei der Steuerung der Straßenbeleuchtung über die nun schon bekannten Bauteile: Messen Sensoren keinen Verkehr von Fußgängern oder Autos, dimmen sie Laternen oder schalten sie gleich ganz ab und helfen so beim Energiesparen. Intelligente Parksysteme sind mit der schmalbandigen Technik ebenfalls möglich, wenn Sensoren kleinräumig Informationen über freie und besetzte Parkplätze via Konnektoren etwa an elektronische Systeme weitergeben, die den Verkehr über Aktoren flexibel und damit effizienter und umweltschonender leiten. Und Mülltonnen könnten einmal die Woche ihren Füllstand melden und die Müllabfuhr erst dann bestellen, wenn die Tonne voll ist.

Gerade das letzte Beispiel zeigt, warum aufwendige Technologien für bestimmte Szenarien einfach überdimensioniert sind. Hier ist NarrowBand IoT die deutlich bessere Alternative und leistet insgesamt einen wichtigen Beitrag dazu, aus unseren Städten die Smart Cities von morgen zu machen.

Smart Industry: Internet der Dinge in Produktion und Logistik

NarrowBand IoT bietet sich auch für Unternehmen an, die das Konzept des Internet der Dinge interessant finden, aber aus Kostengründen eigene und aufwendig verwaltete IT-Infrastrukturen scheuen. Hier gibt es eine ganze Reihe von Szenarien. So lassen sich zum Beispiel in Lagerhallen Waren auf Paletten mit NB_IoT-Modulen leicht verfolgen und lokalisieren. Damit wird eine deutlich effizientere Lagerverwaltung möglich.

Über die vier Wände eines Unternehmens hinaus erlaubt die schmalbandige Verbindung zum Beispiel das Tracking von Containern, die nicht ständig, aber in einer überschaubaren Taktung ihren aktuellen Standort melden. Und – eine Nummer größer: Öl- und Gaspipelines können zur Überwachung mit Sensoren ausgestattet werden, die wichtige

Informationen zu Druck und Durchflussmenge melden, um etwaige Lecks zu erkennen. Und im industriellen Internet der Dinge (IIoT) lässt sich das häufig angeführte Szenario der vorausschauenden Maschinenwartung („Predictive Maintenance“) über energiearme Sensoren und Datenübertragung sehr viel einfacher realisieren als über selbst betriebene Breitband- oder drahtlose Netze. Allerdings bleibt bei unternehmenskritischen Prozessen das generelle Problem von Funknetzen erhalten: Signale können prinzipiell durch externe Störungen („Jamming“) unterbrochen werden und erreichen damit nicht für jeden Anwendungsbereich die notwendige Zuverlässigkeit. Aber dafür wird es voraussichtlich im Rahmen des Ausbaus von 5G Lösungen geben.

Die Zukunft: NarrowBand IoT ebnet der Mobilfunktechnik der 5. Generation (5G) den Weg

Auch wenn NB-IoT noch auf die Mobilfunktechnik der 4. Generation (LTE) aufsetzt, gilt die Technologie bereits heute als Einstieg in die leistungsfähigen 5G-Netze, für die schon bald die Versteigerung der Funklizenzen durch die Bundesregierung begonnen werden wird.

In 5G-Netzen werden spezialisierte Teilnetze, so genannte Slices, zur Verfügung gestellt, die möglichst gut auf die Anforderungen der jeweiligen Anwendungen angepasst sind. Das Slice für IoT in Mobilfunknetzen wird als „Massive Machine Communication“ bezeichnet. Es unterstützt bis zu einer Million Geräte pro Quadratkilometer Fläche(!). Zudem können solche Geräte bis zu zehn Jahre unabhängig von einer externen Stromversorgung agieren.

Schon diese beiden Daten machen deutlich, wie sehr sich NB-IoT für nahezu beliebige unaufwendige Szenarien rund um das Internet der Dinge anbietet, wenn nicht sogar aufdrängt. Gleichzeitig öffnet 5G in naher Zukunft das Mobilfunknetz aber auch für energie- und datenhungrigere Anwendungen: 5G wird eine um den Faktor 100 höhere Datenrate als heutige LTE-Netze ermöglichen, im Maximum also bis zu 10.000 MBit/s, es hat eine rund 1.000fach höhere Kapazität und kann weltweit 100 Milliarden Mobilfunkgeräte gleichzeitig ansprechen – und das je nach Slice bei extrem niedrigen Latenzzeiten von bis zu einer Millisekunde. Diese an sich schon beeindruckenden Werte werden durch die Energiebilanz noch getoppt: Pro übertragenem Bit beträgt der Energieverbrauch gerade einmal 1/1000 des bisherigen Energieeinsatzes, so dass sich in der Summe der Stromverbrauch für das IoT-Netz um satte 90 Prozent reduzieren lässt.

Fazit: Das bisherige Internet der Dinge über Breitbandnetze und die Cloud war in den vergangenen Jahren bereits ein echter Game Changer in der Debatte um die Möglichkeiten moderner

Technologien. Aber erst mit dem schmalbandigen, fast allgegenwärtigen und energiearmen Narrow-Band IoT wird die Vernetzung einer beliebigen Zahl von Alltagsgegenständen, Produktionsmitteln und Sensoren tatsächlich mit vertretbarem Aufwand möglich. Das wird uns auf dem Weg zu Smart Homes, Smart Cities und Smart Industries deutlich nach vorne bringen.

Christoph Henkels

Industrial Internet of Things (IIoT): Darauf kommt es an

Bei den Konsumenten haben sich Geräte auf der Basis von Internet of Things (IoT)-Technologien schon etabliert: Sportbegeisterte setzen auf Fitness Tracker – kleine elektronische Geräte, die am Körper getragen werden und gesundheitsrelevante Daten aufzeichnen. Bei technikaffinen Menschen kommen Smart Watches zum Einsatz – schlaue Uhren, die nicht nur die Zeit, sondern viele weitere Informationen anzeigen. Und das ist erst der Anfang: Trends wie Smart Home und Connected Car stehen längst in den Startlöchern.

In der Industrie sind IoT-Technologien noch keine Selbstverständlichkeit. Die 2017 veröffentlichte Studie „Digital Factories 2020“ des Beratungsunternehmens PwC belegt: Erst rund ein Drittel der Industrie-Unternehmen nutzt digitale Technologien

zur Konnektivität und Datenanalyse. In fünf Jahren wird dieser Anteil jedoch schon bei zwei Dritteln liegen. Neun von zehn Industrieunternehmen investieren in die Digitalisierung ihrer Werke. Das Industrial Internet of Things (IIoT) steht vor dem Durchbruch.

Der Kunde im Mittelpunkt

Industrielle Unternehmen aller Branchen – von der Fertigungs- und Prozessindustrie über den Energiesektor bis zur Logistikbranche – haben das riesige Potenzial erkannt und IoT in ihrer Strategie für die Digitalisierung und Industrie 4.0 verankert. Unternehmen konzentrieren sich vor allem auf die Vernetzung von Produktionsanlagen. So lassen sich die Produktionsprozesse auf der Basis von Daten optimieren oder Wartungsbedarfe vorhersagen.

Haupttreiber dieser Entwicklung ist zum einen der Kunde: Durch den Einsatz von digitalen Technologien können die Firmen schneller auf neue Kundenanforderungen reagieren. Zum anderen verbessert der Einsatz von IoT die Effizienz, da die Anlagen z.B. seltener still stehen und damit produktiver sind.

Es mangelt nicht an guten Ideen, sondern...

Mit den klassischen Anwendungsfällen für das IIoT sind die Unternehmen vertraut: Condition Monito-



Andreas Odenkirchen,
Manager bei im
Bereich Technology
Consulting, PwC

Anonym surfen?

 eBlocker® schützt alle Geräte!



Auspacken, anschließen, fertig.

- ✓ Blockiert Online-Werbung & Tracker
- ✓ Browser-Schutz vor Malware & Phishing
- ✓ IP-Anonymisierung
- ✓ Jugendschutz

Jetzt €25 Rabattcode: **digicon25** auf www.eBlocker.com einlösen. Gültig bis 30.6.2018. 

*Gültig für eBlocker Pro und eBlocker Family. Die Barauszahlung des Gutschein-Gegenwertes und die Kombination mit anderen Preisnachlässen, Gutscheinen oder Rabatten sind ausgeschlossen. Der Rechtsweg ist ausgeschlossen.

ring – die Zustandsüberwachung von technischen Anlagen – oder Predictive Maintenance – die vorausschauenden Wartung – sind nur zwei Beispiele von vielen. Allerdings hapert es bei der Umsetzung. Firmen haben zuweilen Probleme, den konkreten Nutzen der Anwendungen zu bestimmen und eine solide Investitionsrechnung aufzustellen.

Sie beschränken sich zunächst auf Strategien und führen Machbarkeitsstudien oder Pilotprojekte durch. Das ist ein guter Weg, um sich der neuen Technologie zu nähern und das Potenzial besser zu verstehen. Denn viele Entscheider in der Industrie tun sich verständlicherweise schwer, größere Implementierungsprojekte für IIoT-Lösungen anzugehen.

Aktuell stehen viele Unternehmen vor zwei konkreten Herausforderungen: die Umsetzung von Data Analytics auf den IIoT-Daten, sowie die Auswahl der geeigneten IIoT-Plattform. Und so kann das erfolgreich gelingen:

1. Kein IIoT ohne Analytics

IIoT-Technologien dienen zunächst einmal nur der Anbindung von technischen Anlagen an das Internet. So lassen sich die Messwerte zentral verfügbar machen und sammeln. Sensoren messen Daten – etwa Schwingungen, Temperatur oder Stromaufnahme einer Anlage – und senden diese Informationen an eine Cloud-Plattform. Fehlt jedoch die tiefe Expertise im Datenmanagement und der Datenauswertung, liefern die gesammelten Daten kaum Mehrwert.

Das zeigt ein Beispiel: Die Zeitreihe eines Schwingungssensors wird an einer Produktionsmaschine visualisiert. Nur ein erfahrener Techniker kann daraus Rückschlüsse auf den Zustand der Anlage ziehen und einschätzen, ob die Maschine heruntergefahren und gewartet werden sollte. Um aus den Daten konkrete Handlungsempfehlungen abzuleiten, braucht es komplexe analytische Modelle.

Datenaufbereitung bindet Ressourcen

Dabei sollten Unternehmen die Ressourcen und Fähigkeiten für eine erfolgreiche Datenauswertung keinesfalls unterschätzen. Es ist sinnvoll, 60 Prozent des Zeitaufwands in einem Analytics-Projekt für die Datenaufbereitung einzuplanen.

Eine besondere Herausforderung ist das Labeling der Daten, also die Kennzeichnung, bzw. Klassifizierung von Datensätzen. Für Predictive Maintenance müssen z.B. die Zeitreihen vor einem Maschinenausfall besonders gekennzeichnet werden, sodass intelligente Algorithmen aus diesen Datensätzen Muster lernen können. Diese Muster dienen dann als Frühwarnindikatoren für zukünftige Maschinenausfälle.

Ein weiterer Aspekt, den Firmen häufig übersehen, ist der benötigte Datenumfang. Hier geht es nicht nur um die Menge an Messwerten eines Sen-

sors, sondern auch um die Anzahl an beobachteten Events. Erreichen die Ereignisse – etwa der Ausfall einer Maschine – keine kritische Menge, lassen sich auch keine Machine-Learning-Algorithmen auf Basis der Daten trainieren.

2. IIoT-Plattformen – die Qual der Wahl

Aktuell diskutiert die Industrie zudem angeregt darüber, welche IIoT-Plattform am besten geeignet ist. Im Mittelpunkt dieser Diskussion stehen zwei Aspekte: Zum einen geht es um die IT-Architektur zur Anbindung von technischen Anlagen an Cloud-Plattformen. Zum anderen drehen sich die Überlegungen um die Auswahl der passenden Cloud-Plattform und -Anbieter.

Vielen Unternehmen fällt es schwer, die Unterschiede zwischen den vielen Anbietern zu erkennen und eine fundierte strategische Entscheidung zu treffen. Zumal die Tragweite der Entscheidung groß ist: Die IIoT-Plattform bildet die Basis, auf der digitale Lösungen aufbauen, die wiederum die Kernprozesse der Unternehmen nachhaltig verbessern und automatisieren sollen. Die IIoT-Plattform schafft zudem die Grundlage für ein digitales Ökosystem mit Lieferanten und Partnerunternehmen.

Die Anbieter von IIoT-Plattformen lassen sich vier Gruppen aufteilen:

- 1.) Klassische Softwareanbieter wie Microsoft, IBM oder SAP: Basierend auf Ihrer langjährigen Erfahrung in der Entwicklung von Software-Lösungen für Unternehmen haben sie ihre Cloud-Plattformen modular aufgebaut und nutzerfreundlich gestaltet. Sie bieten ein breites Portfolio an IoT- und Analytics-Software.
- 2.) Jüngere Technologie-Unternehmen wie Google oder Amazon: Sie spielen eine immer wichtigere Rolle im Enterprise-Software-Business und zählen zu den größten Anbietern von Cloud-Infrastruktur. Sie bieten zusätzlich aber auch eigene Software Services für IoT und Analytics in der Cloud.
- 3.) Industrielle Unternehmen wie GE, Siemens oder Bosch: Diese sind zum Beispiel mit speicherprogrammierbaren Steuerungen (SPS) stark in der Industrie verankert. Ihr Fokus liegt auf der Konnektivität von industriellen Maschinen zur Cloud. Sukzessive erweitern sie ihre Cloud Services aber auch um die Visualisierung und Analyse der Daten.
- 4.) Start-ups und IoT-Spezialanbieter: Sie besetzen Nischen und ergänzen das Angebot der drei anderen Anbietergruppen.

Die Wahl kann auch auf mehrere Anbieter fallen

Eine strukturierte Vorgehensweise hilft bei der Auswahl der passenden IIoT-Plattform: Anhand

von einigen Anwendungsfällen lässt sich ein grobes Konzept entwickeln. Daraus können Unternehmen die Kernanforderungen ableiten. Auf dieser Basis können sie die Vor- und Nachteile der verschiedenen Anbieter besser identifizieren und bewerten.

Die gute Nachricht: Unternehmen müssen sich nicht auf einen einzigen IIoT-Anbieter festlegen. Denn Kooperationen zwischen den Anbietern sind mittlerweile eher die Regel als die Ausnahme. In den kommenden Jahren werden sich vermutlich zwei bis drei große IIoT-Plattformen durchsetzen. Und um diese herum wird sich ein Ökosystem aus Partnerunternehmen und Spezialanbietern bilden. Welche Plattformen sich letztlich durchsetzen werden, lässt sich aktuell jedoch noch nicht absehen.

Andreas Odenkirchen

Virtual Reality – Science Fiction von heute

Das relativ neue Schlagwort IoT (Internet of Things) umfasst von Smart City über die Nutzung von Telemedizin, Industrie 4.0 bis hin zum Autonomen fahren ein sehr breites Spektrum an „Dingen“. Ebenso gibt es viele Definitionen und Erklärungen zum Thema Internet of Things.

In komprimierter Form kann also gesagt werden, dass IoT aus einer Gesamtheit von Gegenständen besteht, die wiederum technologische Komponenten wie Mikroprozessoren enthalten und unabhängig durch den Menschen über das Internet miteinander kommunizieren.

Virtual Reality (VR) ist dieser grundlegenden Philosophie sehr ähnlich und teilt ebenso den Ansatz der Verbindung von Realem, also Physischem und dem Digitalen. Die

Herangehensweise ist jedoch eine etwas andere. Während bei IoT versucht wird, die reale Komponente auf digitalem Wege mittels Technologie zu beeinflussen so wird bei Virtual Reality dieser Ansatz invertiert. Der Zugang zu einer digitalen bzw. virtuellen Welt wird hierbei über Head Mounted Displays (HMD's), oder auch VR-Headsets genannt, ermöglicht. Eine, auf einem Smartphone basierende, Variante wird in diesem Zusammenhang vernachlässigt, da diese Kombination zwar mehr Nutzer erreicht, jedoch qualitativ und funktional deutlich hinter einem vollwertigen Headset zurückliegt.

Ein adäquates Beispiel für die Kombination von VR und IoT ist die virtuelle Kommunikation oder auch virtuelle Kollaboration genannt. Dabei wird es einer oder mehreren Personen ermöglicht über das Internet in virtueller Form an einem anderen Standort präsent zu sein, zu agieren und zu interagieren. Dies stellt sozusagen die Erweiterung der Audio- und Videotelefonie dar. Der Term Erweiterung wurde bewusst gewählt, da ein Ersatz gegenwärtig nicht

möglich ist und auch unnötig sein kann, wenn z.B. nur einen kurzen Sachverhalt geklärt werden muss.

Die digitale Repräsentation des Nutzers erfolgt über sogenannte Avatare. Diese Avatare können verschiedenste Formen annehmen. Sie reichen von Kopf oder Torso basierten Varianten, Ganzkörper Avatare, Avatare mit realem Gesicht (z.B. gescannt oder fotografiert) bis hin zu Comic Lösungen wie sie aktuell im Bereich Social Media zu finden sind. Je realer die Verkörperung sein soll, also eine funktionierende Gesichtsmimik, Gesten, bei denen einzelne Finger simuliert werden oder Pupillenbewegung etc., desto mehr wird ein Zusammenspiel verschiedenster Technologien nötig.

Spätestens jetzt wird klar auf welcher Stufe wir uns gegenwärtig im Hinblick der technologischen Entwicklung befinden.

Anbieter wie HTC (Vive), Oculus (Rift), Pimax (8K), Leap Motion und andere arbeiten an den verschiedensten Neuerungen und Erweiterungen um die technologischen Hürden zu reduzieren. Unter anderem sind HMD's mit höherem Tragekomfort durch bessere Balance der Komponenten, leichtere und dünnere Materialien angekündigt. Handtracking Lösungen, die Controller obsolet werden lassen, Pupillentracking, verbesserter drahtloser Übertragung, neuartigen Renderverfahren wie z.B. Foveated Rendering bei dem die signifikanten Details auf einen kleinen fokussierten Bereich beschränkt werden, komplett autarke Headsets, die es ermöglichen, ohne externe Sensoren oder Computer zu funktionieren sowie eine höhere Auflösung sind ebenfalls angekündigt.

Diese Neuerungen sind auch zwingend nötig, um in den verschiedenen Bereichen einen deutlicheren Mehrwert zu generieren und den Markt stärker und schneller wachsen zu lassen. Gerade bei virtuellen Meetings und Produktbesprechung kommt es auf die exakte Darstellung von Materialien an, auf eine tiefere Immersion durch realistische Avatare und intelligenten Lösungen für die Simplifizierung der Nutzungs- und Interaktionsmöglichkeiten.

Anwendungskombinationen sind dabei sogar der logische Weg. So können auf der einen Seite Produkte international abgestimmt werden, ohne Businessreisen durchzuführen zu müssen und auf der anderen Seite kann das Personal über verschiedene Standorte hinweg auf gleichbleibendem Niveau geschult werden. Hinzu kommen Vorteile hinsichtlich risikoreicher Schulungen wie z. B. an einem Schmelzofen. Es können vorab Handgriffe erlernt werden, ohne einem realen Risiko ausgesetzt zu sein. Neue Operationsmethoden können nicht nur am Bildschirm betrachtet, sondern anhand eines Trainings an einem digitalen Modell erprobt werden. Es ist nicht schwer sich vorzustellen, dass solche Methoden komplett in die virtuelle Realität verlagert



Klaus Jaworski,
Co-Founder und
Geschäftsführer,
VSPACE GmbH

werden könnten und somit standortunabhängige Behandlungen durch einen Verbund aus menschlicher Expertise und maschineller Präzision ermöglichen.

Virtuelle Konfiguratoren bieten in Industrie und Handel einen besonderen verstärkten Nutzen. Die gesamte Produktpalette eines Unternehmens auf 3 mal 3 Meter darzustellen ist in der realen Welt oft nicht realisierbar. In der virtuellen Welt durchaus möglich. So kann beispielsweise im Autohaus das gewünschte Modell zusammengestellt werden ohne das das Auto physisch verfügbar sein muss. Wohnungen, Häuser und ganze Fabriken können virtuell begehbar sein, ohne vorher auch nur den Grundstein legen zu lassen. Ein Küchenplaner kann die neue Traumküche nicht nur an einem Laptop vorführen, sondern eine virtuelle Begehung ermöglichen. Das alles in Echtzeit und mit der Option das gesamte Umfeld ebenfalls zu konfigurieren.

Vielen Unternehmen ist der enorme Mehrwert noch nicht ganz ersichtlich, da gelinde gesagt die Erfahrung fehlt und viele Beispiele oft nach Science-Fiction klingen. Aber was ist Sci-Fi? Oft dargestellt als eine Zukunftstechnologie die, der jetzigen überlegen ist und wie Magie wirkt. Gerade in Bezug auf den, immer mehr an Bedeutung gewinnenden, digitalen Wandel sollte untersucht werden, inwieweit die eigenen Unternehmensprozesse mit Virtual Reality optimiert werden können, da diese Technologie ohne Zweifel ganze Branchen revolutionieren wird.

Klaus Jaworski

Mit Blockchain-Technologie bereit für das Internet of Things

Blockchain-Technologie ermöglicht neue und effizientere Geschäftsmodelle für Unternehmen

Nur wenige Unternehmen verstehen das Potenzial von Blockchains – und vertun so die Möglichkeit, wichtige Weichen für den langfristigen Erfolg zu stellen. Dabei sagt nicht nur IBM-Chefin Virginia Rometty, dass Blockchain für Transaktionen so wichtig sein wird wie das Internet für die Übermittlung von Informationen. Bedenkt man, dass nahezu jedes Unternehmen von schnellen und reibungslosen Transaktionen und dem Internet of Things abhängig ist, wird schnell klar, wie groß das Potenzial ist – und die Notwendigkeit, jetzt zu handeln.

Noch ist der Begriff Blockchain den meisten vor allem als die Technologie bekannt, die hinter Kryptowährungen steckt. Doch Blockchains können viel mehr – auch im Hinblick auf das Internet of Things. Einige Unternehmen sind deshalb bereits dabei – im Rahmen ihrer Geschäftsstrategien – erste Prozesse auf Blockchain-Technologie umzustellen. Hat man die Vorzüge von Blockchains in Unternehmen erst einmal verstanden, wird auch schnell klar, wieso das so ist. Mit einer Blockchain können gänzlich

neue Prozesse und Geschäftsmodelle geschaffen, aber auch bereits bestehende Abläufe signifikant schneller, besser und günstiger realisiert werden. Bei Blockchains von einer reinen Zukunftstechnologie zu sprechen, wäre also irreführend.

Letztlich macht es keinen großen Unterschied, welche Waren und Güter gehandelt werden – wie sich etwa bei der TUI Group zeigt, die mittels Blockchain ihre Bettenauslastung über Ländergrenzen hinweg optimiert. Das Prinzip und der Ansatz, Blockchain-Technologie einzusetzen, ist in jedem Fall der richtige Weg in eine noch erfolgreichere Zukunft. Denn gerade in Anbetracht des Internet of Things (IoT) oder auch des zukünftigen Internet of Everything (IoE) ist es sinnvoll, Systeme und Prozesse einzuführen, die – ohne den Bedarf Dritter – untereinander Informationen, Waren oder Finanztransaktionen durchführen können. Denn der dezentrale Ansatz von Blockchains stellt Vertrauen und Prozesse auf Technologieebene her. Damit werden sie nicht mehr wie bisher zwischen Systemen und Instanzen benötigt.

Blockchains arbeiten nach einem dezentralen Prinzip, bei dem alle Teilnehmer Informationen nach den gleichen Regeln verifizieren. Hierbei werden Transaktionen überprüft, bestätigt sowie in Blöcken zusammengefasst und hintereinander unveränderlich verkettet. Durch die dezentrale und transparente Struktur können diese Transaktionen sicherer und effizienter gestaltet werden. Dadurch werden die Daten fälschungssicher und der Datenaustausch sicherer. Mit Hilfe von Blockchains lassen sich Informationen austauschen, Verträge und Vereinbarungen abschließen und Zahlungen sicher durchführen – und das alles ohne die Einbindung Dritter wie beispielsweise Zwischenhändler. Verträge, die per Blockchain geschlossen worden sind, können jederzeit nachvollzogen werden und sind manipulationssicher. Angesichts dieser Vorzüge vergleicht Virginia Rometty, CEO von IBM, Blockchain sogar mit der Einführung des Internets: „Die Blockchain ist für Transaktionen das, was das Internet für Informationen war“.

Übergeordnete Strategie ist unabdingbar

Als Lösungsanbieter wissen wir aus praktischer Erfahrung, wie wichtig es ist, sich auf strategischer Ebene mit der Blockchain-Technologie und der Digitalisierung im Allgemeinen aktiv zu befassen. Ebenso wichtig ist es dann jedoch, dass man sich im jeweiligen Unternehmen über relevante Use Cases Praxiserfahrung in ersten Projekten aneignet, um die neue Technologie und den Umgang mit ihr besser zu verstehen. Das gilt sowohl für die IT- als auch für die Business-Seite. Innovationen werden so nicht nur abstrakt diskutiert, sondern erlebt und völlig neue Geschäftspotentiale geschaffen. Hierbei

unterstützen wir unsere Kunden aktiv über die Analyse bis zur Realisierung, um mit ihnen relevante Use Cases zu identifizieren und in ersten prototypischen Entwicklungen gemeinsam umzusetzen. Der Vorteil ist der praktische Wissensaufbau und, bei der Umsetzung von geschäftsrelevanten Use Cases, gleichzeitig auch das Schaffen von Mehrwerten. Nach den ersten prototypischen Entwicklungen unterstützen und betreuen wir unsere Kunden weiter bei der Realisierung und dem Betrieb ihrer Digitalisierungsprojekte.

Industrien, die in ihrem Kerngeschäft im großen Maße von Transaktionen leben, werden nicht darum herumkommen, sich mit den Möglichkeiten von Blockchains und der Digitalisierung auseinanderzusetzen. Dazu zählen beispielsweise die Telekommunikations- oder auch Energiebranche, das Gesundheitswesen, die Logistikbranche sowie der Bereich Industrie 4.0 oder auch die Reisebranche. Je früher die einzelnen Unternehmen oder auch Behörden hier aktiv werden, desto größer wird am Ende der Wettbewerbsvorsprung sein. Dasselbe gilt allerdings auch für all jene Unternehmen, die auf den ersten Blick womöglich gar nicht an den Einsatz der Blockchain-Technologie denken.

Abrechnung zwischen E-Autos und Elektro-Tankstellen per Blockchain

Noch herrscht derzeit vielerorts die Ansicht, dass Endgeräte zunehmend in der Lage sein müssen, beispielsweise ein demnächst benötigtes Ersatzteil bei einem Händler einkaufen und über einen Bezahl-dienstleister abrechnen zu können. Das mag im Einzelfall sogar Sinn ergeben. Möglich ist dies jedoch auch direkt über einen öffentlichen Marktplatz basierend auf einer öffentlichen Blockchain – inklusive der direkten Zahlungsfreigabe und des Startens von z.B. Logistikprozessen durch Smart-Contract-Anwendungen. Diesen öffentlichen Marktplatzansatz diskutieren wir aktuell mit einigen unserer Kunden für industrieübergreifende Services.

Beispielsweise könnte die Abrechnung zwischen E-Autos und Elektro-Tankstellen ganz einfach via Blockchain erfolgen. Beide kennen sich untereinander nicht, müssen sich aber gegenseitig vertrauen. Die Leistung muss bereitgestellt und abgerechnet werden. Da Blockchain-Technologie für Smart-Contract-Anwendungen ebenso wie für die Bezahlung per Kryptowährungen genutzt werden kann, liegt die Lösung eigentlich auf der Hand. Denn der Kern einer Blockchain ist ihre jeweilige Kryptowährung. Diese verleihen ihr Stabilität und Sicherheit. Doch das Anwendungsfeld ist deutlich größer, als vielen Unternehmen mitunter bewusst ist.

Solche Lösungen mögen sich für viele Entscheidungsträger in den Unternehmen weiterhin wie Zukunftsmusik anhören. Dass dem nicht so ist, zeigt

sich beispielsweise bei der TUI Group und deren Betten-Management auf Blockchain-Basis.

Sascha Hellermann

1.1.3 Visionen

IoT – eine große Chance für Europa

Der langfristige Erfolg der Unternehmen in Deutschland und Europa hängt stark von ihrer Beherrschung des Internet of Things und dem Industrial Internet of Things ab. Sie sind gut gestartet, dennoch benötigen die Unternehmen Unterstützung von der europäischen Politik.

Unternehmen werden langfristig prosperieren, die es schaffen, wie acatech-Chef Henning Kagermann schreibt, sich „durch das Internet of Things -Daten und -Diensten zu transformieren“. An dieser Stelle ist das große Wort Transformation keineswegs übertrieben. Es bezieht sich schließlich auf sämtliche Unternehmensbereiche und Prozesse sowie auf die Ebenen Kultur, Organisation und Technologie. Zum Teil sind die Veränderungen grundlegend, teilweise beziehen sie sich auf die Optimierung und Automatisierung bestehender Abläufe. Klar ist aber in jedem Fall, dass die Unternehmen nicht abwarten können, sondern die Veränderungen aktiv gestalten müssen. Schon heute herrscht ein starker Konkurrenzkampf um die besten Startplätze in der digitalen Ökonomie. Einige Experten behaupten, dass die besten Plätze bereits von den großen, meistens US-amerikanischen, Playern besetzt sind. In der reinen Internet- und Plattform-Ökonomie mag das zurzeit so aussehen, im IoT- und IIoT-Thema ist das nicht der Fall.

Europäische Unternehmen sind ehrgeizig

Das belegt unter anderem eine Untersuchung der Beratungsgesellschaft Bain & Company mit dem Titel „Finding Europe's Edge in the Internet of Things“. Die Analysten des Beratungsunternehmens fanden heraus, dass in vielen Fällen europäische Unternehmensverantwortliche ehrgeiziger und optimistischer planen, wenn es um die Nutzung und Integration von IoT-Lösungen geht als ihre amerikanischen Kollegen. In einer Umfrage unter 500 Entscheidungsträgern in Europa und den USA erklärten 27 % der Befragten, dass sie gerade IoT-Lösungen implementieren oder bereits eingeführt haben. In den USA sagten das mit 18 % ein Drittel weniger. 25 % der Europäer planen bis 2020 mehrere Use Cases zu implementieren und mit ihren IT-Systemen zu integrieren. In den USA nur 16 %.

Darüber hinaus, so die Analysten von Bain & Company weiter, verfolgen Amerikaner und Europäer offenbar unterschiedliche IoT-Ziele. Unter den



Sascha Hellermann,
Vorstandsmitglied,
COCUS AG



Dr. Thomas Endres,
Vorsitzender des
Präsidiums, VOICE-
Bundesverband der
IT-Anwender e.V.

Entscheidern, die die Möglichkeiten der Kostenreduzierung durch IoT betonen, begeisterten sich 2/3 der Europäer über das Potenzial der Technologie für Qualitätsverbesserungen an bestehenden Produkten und die neuen analytischen Möglichkeiten. In Amerika stufen das nur 1/3 der Entscheidungsträger als Priorität ein. 3/4 der Amerikaner erwarten hingegen, dass ihnen IoT und die dazugehörigen Analysen helfen, Ausschuss zu vermeiden und Inputkosten zu reduzieren. Auf der europäischen Seite erwarten das nur 35 %.

Europäer investieren mehr in IoT

Ein weiterer Unterschied zwischen amerikanischen und europäischen Entscheidern ist laut Bain & Company ihr Sicherheitsbewusstsein. In der alten Welt sehen 39 % mangelnde Sicherheit als eine der wichtigsten Hürden für die Akzeptanz von IoT-Lösungen, in den USA sind nur 27 % dieser Meinung. Das gleiche Bild zeichnet sich im Bereich Compliance ab. Während 22 % der Europäer die Regulatorik als sehr wichtige Barriere erkennen, glauben das nur 8 % ihrer amerikanischen Counterparts. Die Analysten von Bain interpretieren das als Vorteil für die Europäer. Ihr größeres Bewusstsein für Regulatorik und Sicherheit helfe ihnen bei der Entwicklung kosteneffektiver Lösungen, die einer ganzen Reihe unterschiedlicher Regularien entsprechen und deshalb auch von einer sicherheits- und datenschutzsensitiven Kundschaft angenommen werden.

Nicht zu unterschätzen ist ein weiterer Unterschied. Die Europäer widmen dem IoT-Bereich einen größeren Anteil ihres IT-Budgets als die Amerikaner. So planen europäische Autobauer rund 24% ihrer IT-Budgets für IoT ein, in Amerika nur 20. Auch in den Branchen Retail, Fertigung und Bauen geben die Europäer größere Anteile ihrer Budgets für IoT aus.

Deutsche sind technologie- Amerikaner sind marktgetrieben

Auch die acatech-Studie „Industrie 4.0 im globalen Kontext“ vermittelt den Eindruck von einem relativ gut aufgestellten Unternehmen zumindest in Deutschland. Die Studienautoren Henning Kagermann, Reiner Anderl, Jürgen Gausemeier, Günther Schuh und Wolfgang Wahlster (Hrsg.) wollten mit ihrer Untersuchung aus dem Jahr 2016 herausfinden, welche Chancen und Herausforderungen die internationale Zusammenarbeit im Bereich Industrie 4.0 birgt. Sie basiert auf über 150 Interviews und Gesprächen mit Fachleuten aus Deutschland, China, Japan, Südkorea, Großbritannien und den USA. Diese Länder gelten den Autoren zufolge als zukünftig bedeutende Anbieter von Industrie 4.0-Lösungen. Die Studie zeichnet zwar kein vollständiges Bild der europäischen Nationen, aber

sie offeriert Industrie 4.0 Profile von den Ländern, in denen die Experten befragt wurden. Deutschland als führender Wirtschaftsnation in Europa attestieren sie in Sachen Industrie 4.0 bzw. Industrial Internet einen sehr guten Stand. Allerdings sehen die Autoren die „starke Technologieorientierung“ der deutschen Unternehmen nicht ganz unkritisch, weil sie „ökonomische Faktoren und Potenziale wie neue Geschäftsmodelle und intelligente Produkte oftmals“ nachrangig betrachten. Das sei vor allem in den USA anders. „Das Verständnis für Industrie 4.0 ist im Vergleich zu Deutschland (...) sehr viel breiter angelegt.“ US-Unternehmen seien insbesondere an der „Etablierung neuer Geschäftsmodelle und sogenannter Smart Services in Bezug auf das Industrial Internet interessiert. Entsprechend steht der verstärkt technologiegetriebenen deutschen Perspektive eine stark marktorientierte amerikanische Denkweise gegenüber.“

Die Empfehlungen der Autoren an die deutschen Unternehmen lassen sich sehr gut auf ganz Europa anwenden: Aktive Mitgestaltung der weiteren Entwicklung von Industrie 4.0 auf internationaler Ebene; Anbieten innovativer technischer Lösungen für hochflexible Wertschöpfungsketten, sowie sich Einbringen in die weltweiten Bemühungen um Standards und Normen. Außerdem raten die Autoren den großen Unternehmen, Produkte und Lösungen mit offenen Schnittstellen zu priorisieren. Das werde Ihnen die Verarbeitung der großen Datenmengen erleichtern, die aus dem IoT-Einsatz resultieren. Außerdem versetzen offene Systeme auch mittelgroße Unternehmen in die Lage, eigene Lösungen in die großen Plattformen zu integrieren. Auf diese Weise kann die Wirtschaft auf sehr viel breiterer Basis von IoT profitieren.

Die Mühlen der EU-Politik mahlen zu langsam

Doch nicht nur die Unternehmen, auch Politik und Verbände wie VOICE – Bundesverband der IT-Anwender oder der europäische Verband der Digital-Entscheider EuroCIO spielen eine gewichtige Rolle, wenn es darum geht, IoT in Europa zum Erfolg zu machen.

Die EU-Politik, allen voran die EU-Kommission mit Ihrem für den Digitalen Binnenmarkt zuständigen Vize-Präsident Andrus Ansip, der Digital Kommissarin Mariya Gabriel und dem EU-Science and Research Chief Carlos Modeas sind gefragt. Hauptsächlich in ihren Händen liegen die Aufgaben, einen gemeinsamen rechtlichen Rahmen für die Digitalisierung in Europa festzulegen, die Förder- und Forschungsgelder in die richtigen Bahnen zu lenken (Nachfolge von Horizon 2020 zum Beispiel) und Bildungspolitiker auf nationaler Ebene dabei zu unterstützen, das Digitale in Aus- und Weiterbildung zu verankern.

Es ist keine Frage, die EU-Kommission hat erkannt, dass Digitalisierung und IoT beherrscht werden müssen, um den europäischen Ländern auch in Zukunft wirtschaftlichen Erfolg zu sichern. Die Zahl der Projekte und Initiativen auf EU-Ebene ist beeindruckend. Doch die Ergebnisse lassen bisher nicht wirklich aufhorchen. Insgesamt scheinen die Mühlen der europäischen Politik zurzeit viel zu langsam zu mahlen, um mit den rasanten Entwicklungsschritten der Digitalisierung mithalten zu können. Die Verantwortlichen machen eher den Eindruck, hinter den Entwicklungen herzulaufen – zum Beispiel in Sachen EU-DSGVO, im Urheberrecht oder auch in der Schaffung besserer Investitionsrahmenbedingungen für innovative Start-ups, die zum Beispiel in den USA für einen großen Teil der Innovationen im Bereich Digitalisierung sorgen.

Agile Methoden könnten Politik beschleunigen

Natürlich ist es für eine so große Organisation wie die EU-Kommission, die viele zum Teil sehr unterschiedliche Interessen ausgleichen muss, nicht einfach, Rahmenbedingungen für die Digitalisierung und IoT zu schaffen, für Veränderungen und Entwicklungen also, die noch keineswegs auf breiter Ebene verstanden und deren Auswirkungen noch nicht abzusehen sind. Allerdings sollte sie versuchen, nicht nur mit traditionellen Politik- und Bürokratiemethoden den Herausforderungen der Digitalisierung zu begegnen. Vielleicht können hier aus der Wirtschaft adaptierte Methoden wie Design Thinking oder auch agile Entwicklung – agile politics quasi – helfen, schneller bessere Ergebnisse zu erzielen. Um die nötige Beschleunigung tatsächlich zu erreichen, sind allerdings agile Methoden nicht genug. Die Verantwortlichen müssen sich auch viel stärker auf die Wirkung ihrer Gesetze und Maßnahmen fokussieren, also besser einschätzen, welche Weichen zu stellen anstatt nur zu wissen, wie man sie von Stellung A nach B bewegt.

Damit Unternehmen die Herausforderungen von IoT- und Digitalisierung erfolgreich meistern und damit den wirtschaftlichen Erfolg der europäischen Gemeinschaft mit sichern können, sollte sich die EU-Kommission, aber auch die nationalen Regierungen mit folgenden Punkten intensiv auseinandersetzen:

- Beschleunigte Entwicklung des digitalen Binnenmarktes.
- Die Stärkung der Start-up-Szene über die Hotspots in London, Berlin und Stockholm hinaus durch den Ausbau des European Investment Fonds
- Die Fortführung von Research- und Innovationsprogrammen wie Horizon 2020.
- Die Förderung internationaler Standards und Normen.

- Ausdehnen der Förderung von Security-Forschung.
- Die Stärkung von digitaler Bildung und Weiterbildung.
- Weiterhin selbstbewusst in Sachen Datenschutz und Privacy-Gesetzgebung agieren.
- Die stärkere Einbeziehung von Anwenderunternehmen in Forschungs- und Innovationsprogramme der EU.
- Die stärkere Einbeziehung der Bürger, um sie auf die bevorstehenden Veränderungen besser vorzubereiten.

Die Rolle der Anwenderverbände wie VOICE und EuroCIO in Sachen Digitalisierung und IoT ist in erster Linie die des Kommunikators und Interessenvermittlers. Sie stehen dabei ganz klar auf der Seite der Anwenderunternehmen und müssen sie unterstützen beim Wissenserwerb, durch die Schaffung von digitalen und analogen Austauschplattformen sowie durch die Kommunikation von Best Practices. Darüber hinaus sollten Anwenderverbände mit dafür sorgen, dass Unternehmen Schritt halten können mit den anstehenden Veränderungen. Dazu gehören auch der Kampf für faire Markt- und Lizenzbedingungen sowie für ausreichende und kluge Rahmenbedingungen, die einer erfolgreichen Digitalisierung in Europa zumindest nicht hinderlich sind. VOICE und EuroCIO haben die Aufgaben angenommen und arbeiten erfolgreich an ihrer Umsetzung. Immer mehr Unternehmen erkennen das und werden zu Mitgliedern. Dr. Thomas Endres

Der Weg zur digitalen Transformation

Auf dem Weg ins Büro blieb ich an einer Ampel stehen, die nur drei Autos durchließ, bevor sie wieder rot wurde. In meiner Frustration fragte ich mich, wer sich so etwas ausgedacht hatte und wie es funktioniert, das heißt welche Farbe führt. Nach einer kurzen Suche erfuhr ich, dass vor der Erfindung der elektrischen Ampel Verkehrsoffiziere den Verkehrsfluss in Großstädten kontrollierten. Sie lenkten manuell den Fußgängerverkehr sowie den Kutschenverkehr an Orten wie London Bridge und anderen hochfrequentierten Straßen. Dies war von mindestens 1722 bis 1912 der Fall, bis ein Polizist in Salt Lake City, Utah/USA, die rot-grüne elektrische Ampel erfand. Er automatisierte und transformierte sozusagen digital einen Prozess, der seit fast 200 Jahren existierte.

Grün vs. rot

Im Geschäftsbereich gibt es eine ähnliche Situation. Seit einiger Zeit stellt sich die Frage, wer die digitale Transformation anführt. Ich sehe die IT als grünes Licht und die Branche als rotes Licht. Beide sind gleichwertig, aber beide möchten die Kontrolle der digitalen Transformation übernehmen. Wie bei einer

Ampel, sollten beide zusammenarbeiten, um ihre Organisation digital zu transformieren.

Historisch gesehen war der CIO die Person, die die Bedeutung der Transformation in Unternehmen erkannte. Als Systemfachmann war er mit der Suche nach Technologien vertraut, die Unternehmen dabei unterstützen, Arbeitsprozesse effektiv und effizient zu gestalten. Er war das grüne Licht, das den Verkehr der digitalen Transformation in Gang brachte.

Im Laufe der Zeit änderten sich die Geschäftsanforderungen und der CIO trug oft mit strategischen Initiativen dazu bei, den Unternehmensbetrieb effizienter zu gestalten. Doch es fehlte an Technologien, die Führungskräften helfen konnten, ihre Arbeit effektiver zu erledigen. Beispielsweise hilft ein effizientes Cloudspeichersystem Unternehmen, Kosten zu sparen, aber es kann Führungskräften keinen Einblick in einen bestimmten Satz von Kundendaten geben, um Kunden länger zu binden. So wurden Führungskräfte zum roten Licht. Sie bremsten den CIO aus, damit diese Geschäftsanforderungen erkennen, deren Optimierung neben der Effizienz auch der Unternehmenseffektivität zugutekommt. Die rote Ampel ist entscheidend, um sicherzustellen, dass neue Technologien nicht nur die Betriebskosten, sondern auch das Endergebnis verbessern.

Die Führung

Rotes und grünes Licht legen fest, welche Autos durchgelassen werden. In ähnlicher Weise müssen Branche und IT bestimmen, welche Marktentwicklungen sie in ihrem Unternehmen zulassen. Die treibende Kraft hinter der digitalen Transformation ist die Kommerzialisierung der Technologie. Mitarbeiter wissen oft genau, was sie brauchen, um effektiver arbeiten zu können. Sie wissen, was möglich ist, weil sie die Technologie auf ihren Mobiltelefonen erleben und erwarten die gleiche Erfahrung bei Geschäftsanwendungen. Denn auch sie haben es mit einer Flut von Daten in Form von Instant Messaging, E-Mail, Berichten, Websites und mehr zu tun.

Die IT-Abteilung hat in den letzten 25 Jahren massiv in die E-Mail-Kommunikation investiert. Doch für viele waren E-Mails nicht effizient. Die Form von E-Mails macht das Lesen zu lang und die Datenflut, die sie erhalten, ist schwer zu erfassen. Deshalb investierte IT in die Chat-Kommunikation. Doch das einzige, was sich wirklich änderte, war, dass die Mitarbeiter kürzere E-Mails schreiben konnten, die sofort verschickt wurden. Als Folge davon implementierten einige Branchenführer Collaboration-Software, die kürzere Nachrichten mit der Option, Dokumente, Projektmanagement und vieles mehr einzubinden, ermöglichte. Die mobile App erlaubte dies jederzeit und von jedem Ort aus. Das ist jedoch immer noch nur evolutionär. Digitale Transformation würde viel mühselige Arbeit

automatisieren und Informationen für effektive Entscheidungen bereitstellen, anstatt einfach nur die Kommunikation effizienter zu gestalten.

Schnittstellen

Bei erfolgreichen Digitalisierungsinitiativen habe ich immer wieder festgestellt, dass der CIO zum Vorreiter für die Geschäftsanforderungen wird. Der CIO bespricht in regelmäßigen Abständen mit den einzelnen Geschäftsbereichen, wie sie ihre Prozesse effektiver gestalten können. Mitarbeiterbefragungen und interne Analysen gehören auch dazu. Die wichtigste Frage, die ein CIO stellen sollte, lautet: „Warum machen Sie das so?“. Sobald er den notwendigen Handlungsbedarf feststellt, kann das klassische Konzept der IT umgestaltet und die eingesetzte effiziente Technologie verwendet werden, um effektive, digital transformierte Geschäftsprozesse zu entwickeln. Auf der anderen Seite der Kreuzung werden sich die Führungskräfte mit dem CIO auseinandersetzen, um Prozesse zu identifizieren, die digital transformiert werden können. Sie helfen dabei, ineffiziente Arbeitsabläufe zu beheben und neu zu überdenken, um die Art und Weise, wie Mitarbeiter Geschäfte abschließen, innovativ zu gestalten. Diese Prozesse unterstützen den CIO bei der Priorisierung von Projekten und bieten Ressourcen für Aktivitäten, die von ihren Teams effektiv bearbeitet werden können. Führungskräfte werden dazu beitragen, Innovationen voranzutreiben. Wenn Entwicklung und Betrieb aufeinandertreffen, werden Geschäftsprozesse besser, schneller und erfolgreicher.

Traffic Flow

Wer sollte also bei der Digitalisierung eine führende Rolle spielen? Die Antwort ist: Beide. Rotes und grünes Licht brauchen einander. Nur mit beiden kann das Unternehmen die Marktentwicklung steuern. CIOs und Führungskräfte müssen an der Schnittstelle von Entwicklung und Betrieb zusammenkommen, um erfolgreich zusammenzuarbeiten und die digitale Transformation in ihren Organisationen zu leiten.

Georg Goller

Warum künstliche Intelligenz dem Internet of Things zum Durchbruch verhelfen wird.

Das Internet of Things (IoT) ist einer der Trends, dem zwar seit mehreren Jahren ein großes Potential zugeschrieben wird, der sich bislang aber nicht in der breiten Masse durchgesetzt hat. Es gibt gefühlt mehr Texte über den vernetzten Kühlschrank, der weiß, wann die Milch abgelaufen oder aufgebraucht ist, als Menschen, die ihn tatsächlich benutzt haben. Auch im „Hype Cycle“ von Gartner wird das IoT als Trend geführt, der mit hohen Erwartungen verbunden ist, aber im Moment noch immer hauptsächlich

als Auslöser für Innovationen bewertet wird.

Um das Potential des IoT richtig einzuschätzen sollte das IoT jedoch – ganz im Gegensatz wie das im „Hype Cycle“ gemacht wird – im engen Zusammenhang mit der Entwicklung im Bereich der Künstlichen Intelligenz (KI) betrachtet werden. Denn erst eine intelligente Auswertung und Steuerung von Datenprozessen durch den Einsatz von KI wird der Vernetzung der Dinge zum Durchbruch verhelfen. Seit die Kosten für KI seit kurzer Zeit signifikant sinken und die Anwendungsreife gleichzeitig zunimmt, wird die Wechselwirkung zwischen KI und IoT immer wahrscheinlicher.

Daten bilden die Schnittstelle zwischen IoT und KI

Die vernetzten Dinge liefern Daten in einem bislang ungekannten Maßstab. Dabei spielen diese Daten in zweifacher Hinsicht eine wichtige Rolle. Auf der einen Seite dient die Erhebung der Daten dazu, bestimmte Dinge intelligenter zu machen, als sie es zuvor in ihrem nicht-vernetzten Zustand waren. Beispielsweise der Dash-Button von Amazon, der über einen Sensor wahrnehmen kann, ob er gedrückt wird und diese Information dann in eine Bestellung übersetzt und diese via Internet weiterleitet. In der ein oder anderen Form führen alle IoT-Geräte Echtzeit-Analysen dieser Art durch und nehmen ihre Umgebung wahr. Auf der anderen Seite spielen Daten und Datenanalysen aus der Perspektive der Unternehmen, die vernetzte Produkte herstellen, eine zentrale Rolle beim Erfolg des IoT. Unternehmen müssen durch die Analyse der Nutzungsdaten lernen, wie ihre Produkte tatsächlich eingesetzt werden und wie sie verbessert werden können. Was passiert beispielsweise, wenn ein Kind beim Spielen den Dash-Button 23x hintereinander drückt? Im Gegensatz zu den Echtzeit-Analysen wird hier auch von Post-Event-Analysen gesprochen. Durch den Einsatz von Deep Learning bzw. Machine Learning lassen sich Muster erkennen und analysieren, die dabei helfen, den Gebrauch von IoT-Produkten besser zu verstehen und die damit verknüpften Prozesse besser zu steuern.

KI macht vernetzte Dinge erst intelligent

Viele vernetzte Dinge wie beispielsweise ein smarterer Staubsaugerroboter funktionieren als autarke Einheiten, die jedoch über die Cloud in ein umfassenderes Ökosystem wie ein Smart Home eingebunden werden können. Erst wenn diese Einheiten dazu fähig sind, aus ihrem täglichen Einsatz zu lernen und intelligente Schlüsse zu ziehen, werden sie wirklich zu smarten Dingen. Man spricht hier auch von adaptiver Intelligenz. Im Falle des Staubsaugers könnte das etwa bedeuten, dass er die Wohnung nach und nach kennenlernt und ab einem gewissen Punkt gezielt in die Küche zum Säubern

geschickt werden kann. In diesem Zuge steigt auch die Sicherheit von IoT-Geräten durch die Integration von KI. Denn durch Monitoring und Mustererkennung kann besser zwischen normalem Nutzen und Angriff von außen unterschieden werden.

Das IoT braucht KI

Beim IoT geht es primär um die Erhebung, Auswertung und Nutzung von Daten bei alltäglichen Gegenständen und Dingen. Je besser die Daten ausgewertet und in einen sinnvollen Nutzen übersetzt werden können, desto eher werden auch Unternehmen und Endverbraucher IoT-Geräte anbieten bzw. annehmen. KI bietet die Chance, die Daten, die im IoT-Umfeld anfallen, besser als jemals zuvor zu analysieren. Insbesondere durch Machine-Learning-Algorithmen lassen sich entsprechend IoT-Lösungen besser in vorgegebene Kontexte integrieren, weil sich dadurch einerseits die Echtzeit-Analysen verbessern lassen, aber auch weil sich im Post-Event-Processing wiederkehrende Muster ableiten lassen. Auch eine vor kurzem durchgeführte PwC-Studie endete mit dem Fazit: „Das IoT braucht smarte Maschinen. Es gibt also einen Bedarf an AI.“ Das bedeutet umgekehrt auch: Nur wenn das IoT und KI konsequent zusammen gedacht werden, lassen sich intelligente Lösungen entwickeln, die aus den Daten einen echten, sinnvollen Mehrwert erzeugen.

Michaela Tiedemann

1.2 SICHERHEIT

1.2.1 Herausforderungen

Internet of Things (IoT) – von der Zukunft von Endgeräten bis hin zu ihren Sicherheitsproblemen

Die Vorzüge, die das IoT mit sich bringt sind enorm: Durch die Verknüpfung von Alltagsgegenständen, Maschinen in der Produktion, oder Immobilien mit dem Internet sollen zukünftig maschinelle Abläufe „smarter“ werden. Der automatisierte Datenaustausch zwischen den Geräten erlaubt eine ständige Kontrolle von wichtigen Parametern und eröffnet dabei neue Geschäftsfelder. Die Verbindung all dieser Geräte birgt natürlich ein gewisses Risiko, wenn z.B. ein ungeschütztes Gerät dazu genutzt wird, das Netzwerk eines Unternehmens zu infiltrieren. Eine zentrale Rolle spielt deshalb immer das Thema „Security“, um Daten sicher zu transportieren und vor Angriffen zu schützen. Nur wenn effiziente Sicherheitslö-



Michaela Tiedemann,
Chief Marketing
Officer, Data Science
Beratung



Georg Goller, Area
Vice President
Germany, ServiceNow

sungen implementiert werden, kann das Konzept nachhaltig funktionieren.

Laut dem Technology Researcher Gartner werden bis 2020 25 Milliarden IoT-Devices miteinander verbunden sein und insgesamt 2 Billionen Dollar wirtschaftlichen Nutzen generieren.[1]

IoT bezeichnet die Verknüpfung eindeutig identifizierbarer physischer Objekte (things) in einer Internet-ähnlichen Struktur. In der Regel ist ein Objekt ein eingebettetes System, das Daten über ein Netzwerk übertragen kann und völlig automatisch agiert – ohne, dass menschliche Interaktionen nötig sind.[2]

IoT-Devices stellen deshalb eine riesige Angriffsfläche für potenzielle Hacker dar. Forrester prognostiziert hierzu, dass im Jahr 2017 mehr als 500.000 IoT-Devices einen erfolgreichen Angriff erleiden werden.[3] Das ist alleine schon durch die schiere Anzahl an Geräten und keine bzw. wenige Sicherheitsanforderungen an die Hersteller begründet.

Anlässe und Beispiele für IoT-Sicherheit:

- Das Mirai-Botnetz hat über eine Million „Zombies“ unter seiner Kontrolle, darunter Kameras, Videorecorder und Drucker. Internet Dienste wurden durch DDoS Angriffe unbenutzbar.[4]
- Miele Geschirrspüler mit dem „directory traversal bug“. Geschirrspüler von Miele sind über einen Browser ansteuerbar und durch einen Bug anfällig für Attacken von außerhalb. Hacker konnten diesen ausnutzen (exploiten) und auf sensible Daten des Nutzers zugreifen, indem sie Zugriff auf den Webserver der Waschmaschine erhielten.[5]

Herausforderungen

- Typisch für IoT-Devices sind minimalistische, teilweise proprietäre Betriebssysteme mit wenig Overhead, die nicht durch traditionelles Netzwerkmanagement erkannt und kontrolliert werden können. Zumeist werden alte Linux Distributionen benutzt.
- Aufgrund dessen ist das Thema Embedded Security noch nicht weit verbreitet und die Installation von Agents nicht möglich. Sicherheitslücken können auch nicht bzw. schwer gepatched werden.
- IoT Netzwerksicherheit übersteigt die Komplexität eines herkömmlichen Netzwerks. Das liegt u.a. an einer breiteren Palette an Kommunikationsprotokollen und Standards. IoT-Devices sind noch selten und können nicht automatisch in einer Security-Policy abgebildet werden.
- Der Datenaustausch und die Steuerung von IoT-Devices sollte zusätzlich überwacht und

reguliert werden. Dies sollte z.B. von Steuerungsrechnern und Datenbanken abgesichert werden, welche wiederum mit Next-Generation Endpoint Protection Systemen geschützt werden können.

Lösungsansatz

Trotz der Herausforderungen müssen IoT-Devices in einem Netzwerk sicher betrieben werden.

Unternehmen können durch einen intelligenten Netzwerkaufbau die Angriffsfläche minimieren und ihre Sicherheitsstrukturen durch klare Verantwortlichkeiten effizienter gestalten:

- Empfehlenswert ist die dynamische Segmentierung des Netzwerks (ohne Endpoint Agent oder Supplikant), um das Ausmaß von Sicherheitseinbrüchen zu limitieren. Beispielweise kann ein Unternehmensnetzwerk in verschiedene VLANs (Virtual LAN) aufgeteilt werden. IoT-Devices können ein eigenständiges Segment umfassen und von anderen Segmenten isoliert werden.
- Eindeutige Verantwortlichkeiten über die gesamte Sicherheitsinfrastruktur, d.h. von der Beschaffung der Geräte bis hin zur Planung, Implementierung und Betrieb.

Für eine umfassende Absicherung müssen zusätzlich geeignete Sicherheitslösungen implementiert werden:

- Einsatz von Sicherheitslösungen, die dynamisch das Netzwerk befragen und somit alle vorhandenen Geräte des Netzwerks identifizieren und kategorisiert. Hier bietet z.B. ForeScout CounterAct einen agentenlosen Ansatz, um Geräte innerhalb des Netzwerkes zu erkennen und zu klassifizieren. Dies geschieht durch automatisierte Policies.
- Durch verhaltensbasierte Netzwerkanalyse und die Überwachung der Kommunikation zwischen den Endpoints (sog. Flow-Analyse) können verdächtige Verhaltensweisen zwischen den Endpoints (z.B. von nicht verwalteten Geräten) im Netzwerk erkannt werden. Hier bietet Vectra Networks eine spezielle Appliance an, die sich einfach in ein Netzwerk implementieren lässt und eigenständig durch künstliche Intelligenz Bedrohungen ermittelt.
- Nutzung intelligenter Incident Response Plattformen durch Orchestrierung aller Sicherheitskomponenten wie Firewall, SIEM (Security Information and Event Management) und Endpoint.
- Überwachung, Prüfung und Protokollierung des Netzwerks durch eine Next-Generation Firewall. Im Gegensatz zu einer herkömmlichen Firewall analysieren Next-Generation Firewalls detailliert den Datenstrom und können

z.B. auf User- und App-Basis Zugriffe auf das Netzwerk beschränken.

Checkbox:

- Teilen Sie Ihr Netzwerk in verschiedene Segmente auf, um zu verhindern, dass Angriffe Ihr gesamtes Netzwerk betreffen!
- Nutzen Sie intelligente Sicherheitslösungen, um alle IoT-Devices zu überwachen und verdächtige Verhaltensweisen schnell zu erkennen.
- Überwachen Sie Ihr Netzwerk durch eine Next-Generation Firewall, die Ihr Unternehmensnetzwerk effizienter beschützen kann als eine herkömmliche Firewall.

Der Rückgriff auf einen erfahrenen Security-Provider kann Unternehmen zusätzlich dabei unterstützen, eine passende Sicherheitslösungen zu finden und implementieren.

Markus Reiniger

Referenzen: [1] Vgl. <http://www.gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise/>, aufgerufen am 03.04.2017. [2] Vgl. <http://www.gartner.com/it-glossary/internet-of-things/>, aufgerufen am 03.04.2017. [3] Vgl. <https://internetofbusiness.com/iot-security-breach-2017-forrester/>, aufgerufen am 03.04.2017. [4] Vgl. <https://www.golem.de/specials/mirai/>, aufgerufen am 03.04.2017. [5] Vgl. https://www.theregister.co.uk/2017/03/26/miele_joins_internetofst_hall_of_shame/, aufgerufen am 03.04.2017.

IoT-Geräte: Wenn Cyber Security für Kunde und Marke zum kritischen Faktor wird

Die Allgegenwart des Internets bietet kostengünstige und stetig verfügbare Konnektivität für Geräte, Systeme und Prozesse. Die so generierten Verbraucher- und Nutzerdaten erkennen immer mehr Hersteller als eigenen Wert und Basis neuer und gewinnbringender Geschäftsideen. Zugleich ist es für viele Nutzer normal, persönliche Informationen gegen vermeintlich „kostenlose Dienste“ zu tauschen. Sollten sich jedoch Sicherheitsvorfälle ereignen, drohen Geräte-Herstellern inzwischen drastische Strafen, ganz zu schweigen von den Reputationsschäden. Was ist Herstellern zu raten, die einen Imageschaden ihres Unternehmens oder Rechtsstreit vermeiden möchten? „Auf jeden Fall die Bedrohungen und Risiken monitoren und entsprechend handeln“, sind Nigel Stanley und Mark Coderre von TÜV Rheinland überzeugt. Die Experten für Cyber Security zeigen den aktuellen Status Quo zu IoT und Cyber Security und geben strategische Empfehlungen, um Sicherheitsschwachstellen von IoT-Geräten so weit wie möglich zu vermeiden.

Der sinnvolle Einsatz von IoT-Geräten und damit erhobenen Daten kann unseren Lebensstandard und die Produktivität der Herstellung verbessern. Mit den zahlreichen Möglichkeiten von Big Data Analysen – bei denen Daten gezielt auf nützliche Informa-

tionen untersucht werden – eröffnen sich neue und aufregende kommerzielle Möglichkeiten. Grundlage für diese neuen Geschäftsmodelle ist das Internet of Things (IoT) oder auch Internet der Dinge. Immer mehr Hersteller bieten Produkte oder Services, mit denen sich die Vorteile des Internets und des World Wide Webs umfassend nutzen lassen.

Hersteller von Medizingeräten haben bereits früh erkannt, dass das Leben von Patienten und Ärzten durch die Ausstattung von Geräten mit IoT-Funktionalität verbessert werden kann. Gute Beispiele dafür sind die zahlreichen Blutzucker-Messgeräte, die per Smartphone gesteuert werden und Daten via Internet übermitteln. Dadurch wird den Betroffenen der Umgang mit Diabetes etwas erleichtert.

Allerdings hat so mancher Hersteller von Medizingeräten seine Geräte recht übereilt an das IoT angepasst, ohne die damit verbundenen Probleme rund um Cyber Security zu beachten bzw. sie zu lösen. Schwachstellen wie

- mangelhafte oder fehlerbehaftete Soft- bzw. Firmware, die die Sensibilität und Integrität medizinischer Daten bzw. Funktionen nicht adressiert,
 - falsch konfigurierte Netzwerkdienste mit unverschlüsselter Übertragung von Patientendaten,
 - Sicherheits- und Datenschutzprobleme wie die Verwendung schwacher Passwörter oder eine zu weitreichende Vergabe von Berechtigungen für nicht privilegierte Benutzer, die als Einfallstore für Hacker dienen können,
- sind da nur die Spitze des Eisbergs. Eine der bekanntesten Vorfälle im Gesundheitswesen stammt aus 2015. Seinerzeit warnte die US-amerikanische Bundesbehörde für Arzneimittel und Medizinprodukte, Federal Drug Agency (FDA), vor dem Hospira Symbiq Infusion Systems. Über das Krankenhausnetzwerk hätte ein unautorisierter Dritter die Infusionspumpe unter seine Kontrolle bringen und die verabreichte Dosis verändern können. Konkrete Vorfälle waren glücklicherweise nicht bekannt. Vom Markt genommen wurde das Symbiq Infusion System dennoch, weil auch noch andere Schwachstellen aufgetreten waren.

Ein schnelles Aus für ein Produkt gab es in der jüngsten Vergangenheit auch hier in Deutschland: 2017 wurde eine Spielzeugpuppe aufgrund von Sicherheitsbedenken verboten. Die My Friend Cayla-Puppe verwendete eine Spracherkennungstechnologie über einen Service mit Sitz in den USA. Die Daten aus den Tonaufnahmen erwiesen sich als ungesichert und konnten laut Endbenutzer-Lizenzvertrag an Dritte weitergeleitet werden. Das Produkt wurde auf Basis US-amerikanischen Bundesgesetzes Espionage Act vom Markt genom-



Markus Reiniger,
Consultant
IT-Security, iT-CUBE
SYSTEMS AG



Nigel Stanley,
TÜV Rheinland



Mark Coderre,
TÜV Rheinland

men. Bei einem anderen Vorfall waren 2017 zwei Millionen Sprachaufzeichnungen von Kindern, die von CloudPet-Stofftieren aufgenommen wurden, aufgrund einer unsicheren Datenbank zeitweise online für jedermann zugänglich.

Unnötig zu erwähnen, dass es sich in allen Fällen mindestens um geschäftskritische Imageschäden handelte. Was ist Unternehmen zu raten, die solche Fälle vermeiden möchten? Einer der ersten Schritte ist die Integration des IoT-Cyber-Risikos in das Risiko-Register des Unternehmens und die Durchführung einer DICE-Bewertung für alle geplanten Produkte und Services. DICE ist das Akronym für einen inhärenten Risikobewertungsansatz, das für "Dependency" (Abhängigkeit), "Impact" (Auswirkungen), "Complexity" (Komplexität) und "Ecosystem" (Ökosystem) steht und von TÜV Rheinland entwickelt wurde. Entscheidend für die Bewertung eines Systems, Prozesses oder Gerätes gemäß der DICE-Kriterien ist, dass angemessene und kostengünstige Maßnahmen zur Risikobewältigung implementiert werden. Alle Produkte und Services sollten eine DICE-Bewertung durchlaufen und zwar auf Basis eines strategischen Plans. Die Qualifizierung, ab welchem Punkt Sicherheit zu einem wichtigen oder kritischen Faktor für Endverbraucher und die eigene Marke wird, ist auf jeden Fall vital.

Darüber hinaus können Prüfungen und Zertifizierung von IoT-Services einen qualifizierten Nachweis darüber leisten, dass Hersteller personenbezogene Daten ihrer Kunden gut schützen und für den Kunden transparent verarbeiten. TÜV Rheinland etwa bietet ein Produkt- und ein Service-Zertifikat, mit dem Produkthersteller sowie Systemanbieter zeigen können, dass ihr Angebot entsprechend den Anforderungen der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) geprüft wurde. In den IoT-Prüfungen bewertet TÜV Rheinland unter anderem, inwieweit Prozesse und Maßnahmen implementiert sind, um Sicherheitsvorfällen vorzubeugen und gegebenenfalls angemessen reagieren zu können.

Compliance allein macht ein Produkt noch nicht sicher. Erst wenn Hersteller die mit Cyber-Sicherheit verbundenen Bedrohungen und Risiken monitoren und daraus entsprechende Konsequenzen ziehen, können sie sich auf ihre Produktinnovationen konzentrieren – in der Gewissheit, alle erforderlichen Maßnahmen ergriffen zu haben, die der dynamischen Entwicklung auch wirklich Rechnung tragen. Mehr Informationen über das DICE-System und eine Checkliste der wichtigsten Empfehlungen für Hersteller rund um die Cyber Security von IoT-Geräten enthält das Whitepaper von TÜV Rheinland unter dem Titel „Herausforderungen im Internet of Things (IoT)“, das hier herunterzuladen ist.

Nigel Stanley, Mark Coderre

Sicherheitsrisiko Internet of Things

Der große Boom des „Internet der Dinge“ beflügelt auch die Diskussionen über Sicherheitslücken, die mit Internet-fähigen Geräten einhergehen. Wenn sämtliche Maschinen eines Unternehmens, angefangen bei Produktionsanlagen über die Klimaanlage bis hin zum Kopiergerät Daten mit dem Internet austauschen, entstehen neue Einstiegspunkte für Angriffe auf das Unternehmensnetz. Die Abwehr moderner Gefahren gestaltet sich jedoch schwer, da das Thema Sicherheit bisher bei der Herstellung dieser Geräte und Maschinen nicht ausreichend berücksichtigt wurde. Da Hacker-Attacken auf Internet-fähige Geräte und Produktionsanlagen bereits zur Realität geworden sind, tun neue Sicherheitsansätze Not.

Wenn von IoT die Rede ist, sind all jene Geräte im Unternehmenseinsatz gemeint, die intern und extern kommunizieren und aufgrund ihrer IP-Adresse über das Internet erreichbar sind. Die klassischen Bürogeräte wie Drucker, Kopierer, Beamer, das Fernsehgerät im Konferenzraum oder am Empfang zählen dazu ebenso, wie weniger offensichtliche Geräte aus dem Haushaltsumfeld. Darunter fallen Geräte wie Kühlschrank und Kaffeemaschine oder Überwachungskamera, die heutzutage Internet-fähig sind. Zu berücksichtigen sind zunehmend auch Geräte aus dem HVAC-Bereich, wie Heizung, Belüftung und Klimaanlage, sowie Bewegungsmelder oder Beleuchtungssysteme, die mit Intelligenz versehen und per Fernwartung über das Internet oder die Cloud ansteuerbar sind. Darüber hinaus hat in Produktionsanlagen im Zuge der Industrie 4.0 die Zukunft bereits Einzug gehalten mit IP-basierten Maschinen.

Mangelhafte Nachrüstbarkeit

All diese Geräte in einer modernen Büro- oder Produktionsumgebung sind in der Lage, Daten über das Netzwerk auszutauschen oder über das Internet gesteuert zu werden. Allerdings stellt die Internet-Anbindung auch den potenziellen Angriffsvektor dar, da eine Vielzahl dieser Geräte im Entwicklungsprozess nicht mit einer adäquaten Sicherheitsinfrastruktur gegen Attacken von außen entworfen wurde. Denn in Punkto Cyber-Security hinken die Hardware-Hersteller aus Kostengründen hinter den marktüblichen Sicherheitsstandards im PC-Umfeld hinterher. Sie müssen erst lernen, die Sicherheitsfunktionalität in ihre Geräte zu implementieren, um die Gefahr des unerwünschten Zugriffs auf die Geräte und deren generierten Daten zu unterbinden.

Viele einfache Geräte, wie beispielsweise Überwachungskameras, werden möglichst kostensparend produziert und sind dementsprechend nur

mit den Grundfunktionen zur Erfüllung ihrer eigentlichen Bestimmung ausgestattet. Ein nachträgliches Update der Firmware nach Bekanntwerden einer Sicherheitsschwachstelle ist oftmals nicht einmal vorgesehen. Das Sicherheitsbewusstsein bei den IoT-Herstellern sowie bei den Anwendern wächst erst langsam. Immerhin: Die „smarteren“ unter den IoT-Geräten können schon heute durch regelmäßige Firmware-Updates auf einen aktuellen, sicheren Stand gebracht werden.

Damit sind jedoch längst nicht alle Sicherheitsprobleme beseitigt. Denn die Mehrzahl der Internet-fähigen Geräte lässt sich nicht in das herkömmliche IT-Sicherheitskonzept integrieren, das im Unternehmen durch Security-Hardware oder Software-Schutz gegen Internet-basierte Angriffe bieten soll. Im Bereich der Industrieanlagen ist der Herstellungszyklus darüber hinaus so lange, dass diese Geräte nicht mit dem Gedanken der Anbindung an das Firmennetzwerk entwickelt wurden. Der netzwerkbasierte Fernzugriff zu Wartungs- oder Steuerungszwecken wurde oftmals nachträglich implementiert – allerdings ohne dass die Geräte mit der nötigen Sicherheitsinstanz gegen unerwünschte Zugriffe von außen versehen wurden.

Industrie 4.0 öffnet Sicherheitslücken

Werden nun gerade die Industrieanlagen in das Unternehmensnetz eingebunden, kann das mit gravierenden Sicherheitslücken einhergehen. Denn ein Remote Zugriff öffnet vielfach das gesamte Netzwerk für den Zugriff von außerhalb und nicht nur den Zugang auf die Applikation zur Ansteuerung der einzelnen, benötigten Maschine. Die Angriffsfläche auf alle Daten und Anwendungen im Unternehmensnetz erhöht sich deutlich und ist nur durch großen Mehraufwand und Komplexität mit zusätzlichen Sicherheitsvorkehrungen in den Griff zu bekommen. Der von einer Vereinfachung getriebene Wunsch nach Öffnung in Richtung Industrie 4.0 bleibt auf der Strecke, wenn an anderer Stelle der manuelle Verwaltungsaufwand für die IT-Abteilung exponentiell ansteigt.

Ein Umdenken hinsichtlich der Sicherheit ist gefordert. Einerseits hinken die Produktionszyklen gerade im Anlagenbau den modernen Anforderungen hinterher, denn der Sicherheitsaspekt wird bisher nur unzureichend in der Designphase berücksichtigt. Andererseits wächst das Bewusstsein nach erforderlicher Sicherheit beim Zugriff auf die Maschine oder das IoT-Gerät. Um diesen Widerspruch aufzulösen, sind neuartige Ansätze gefragt. Denn gerade in Bereichen, in denen Nachbesserungen in Bezug auf Zugriffsschutz dringender angeht, kann die Cloud wiederum ihre

Stärken ausspielen. Ein Cloud-basierter Security-Ansatz kommt eben ohne komplexe Sicherheitsinfrastruktur vor Ort aus, sondern verlagert diese in die Cloud. Im wahrsten Sinne muss dabei diese in die Cloud. Im wahrsten Sinne muss dabei vollumfänglich „Outside the Box“ gedacht werden, denn halbgeare Lösungen mit „ein bisschen Sicherheit“ verschlimmern die Situation nur und würden neue Angriffspunkte bieten.

Ein möglicher Lösungsweg für IoT-Security

Der Fernzugriff auf Industrieanlagen beispielsweise zu Wartungszwecken sollte aus Sicherheitsgründen nicht mehr von dem mit dem Service betrauten Anwender zur Maschine aufgebaut werden. Er muss vielmehr durch die entgegengesetzte Richtung in die Wege geleitet werden und dementsprechend als ausgehende IP-Verbindung von der Maschine aufgebaut. Da die Anlage bei einem solchen Ansatz nicht im Internet mit geöffneten Ports sichtbar wird, minimiert sich die Angriffsfläche für Angreifer von außerhalb. Lediglich dem autorisierten Anwender oder Dienstleistungsunternehmen wird bei einem solchen Reverse Tunnel-Modell der sichere und granulare Zugriff auf Ebene der einzelnen Anwendung eingeräumt. Eine Ende-zu-Ende Verschlüsselung sorgt für die erforderliche Sicherheit bei der Datenübertragung zur Wartung von Industrieanlagen. Die Policies der Zugriffsrechte werden dabei durch ein zentrales Portal verwaltet und nur genau der eine Anwender erhält den nötigen Schlüssel zum Zugriff. Ein Konnektor, der vor die Anlage oder Maschine geschaltet wird, sorgt bei einem solchen Modell für die sichere Verbindung zwischen der Maschine und dem Anwender, der für die Fernwartung verantwortlich ist.

Unternehmen, die auf das Internet of Things oder auch Industrie 4.0-Vorteile setzen wollen haben also die Wahl: Sie warten ab, bis die Sicherheit bereits vom Hersteller der Geräte und Anlagen im Designzyklus berücksichtigt wird, was allerdings je nach Lebensdauer einen nicht unerheblichen Vorlauf bedeutet. Oder die Organisationen rüsten ihre bestehenden Anlagen mit einem modernen Cloud-basierten Sicherheitsansatz nach und profitieren wesentlich schneller von den Vorzügen der Digitalisierung. Denn auch wenn auf Herstellerseite ein Umdenken bereits eingesetzt hat, werden noch Jahre vergehen, bis Internet-fähige Geräte moderne Sicherheit bereits in der Designphase implementiert haben.

Claus Vaupel

Datenverlust lauert auch im IoT

Datenrettung ist nicht zwangsläufig das Erste, was einem in den Sinn kommt, wenn man an IoT denkt. Doch bei unserer mittlerweile mehrma-



Claus Vaupel,
Manager Sales
Engineering EMEA
Central & Solution
Architect, Zscaler

ligen Teilnahme an Konferenzen und Events zu diesem Thema, konnten wir feststellen, dass es da doch ein paar Anknüpfungspunkte gibt. So stecken natürlich auch in den meisten IoT-Geräten Datenträger für den Betrieb. Das kennt man in großem Umfang auch aus Industriesteuerungen und -anlagen. Von herkömmlichen Speicherkarten bei Einplatinencomputern wie den Raspberry Pis über integrierte Flash-Zellen bis hin zu klassischen Festplatten – die Bandbreite der Speichermedien ist groß. Auch diese Datenträger werden irgendwann defekt, „die Frage ist immer nur wann!“. Dieses Zitat von unserem technischen Leiter Peter Franck hat sich stets bewahrt und wenn es soweit ist, werden oft im Affekt übereilte Handlungen getroffen, die fast immer zu noch größeren Schäden führen.

Zum Thema Konsequenzen nach einem Datenverlust im Bezug auf IoT fällt mir konkret ein Fallbeispiel ein: die Gebäudeautomatisierung in einem Bürokomplex stand still, da die Festplatte Lesefehler hatte. Dies bedeutet, dass mit einem Schlag das Licht nicht mehr auf- und abgedreht werden kann, die Klimaanlage kann nicht mehr bedient werden und die Jalousien nicht mehr rauf- und runtergefahren werden. Diese Liste kann natürlich noch sehr lange fortgeführt werden.

Oder aber ein Hotel dessen Gäste Ihre Zimmertüren mittels Key-Cards nicht mehr öffnen konnten, nachdem der Verwaltungs-PC von einem Ransomware-Trojaner befallen wurde.

Ein weiteres Beispiel wären SmartHomes, die wie manch andere IoT-Geräte nur dann funktionieren, wenn sie nach Hause in die Cloud telefonieren können, da man sie nicht direkt bedienen kann, sondern alles über zentrale Server des Herstellers läuft. In diesen Fällen können die Geräte, Beleuchtung, etc. nur bei bestehender Internetverbindung bedient werden, selbst wenn dein internes (WLAN) Netzwerk ansich noch funktionieren würde.

Man sollte sich also auf jeden Fall immer Gedanken über mögliche auftretende Komplikationen machen, sodass man im Fall der Fälle gerüstet ist und richtig reagieren kann!

Der Autor: Nicolas Ehrschwendner ist Geschäftsführer von Attingo Datenrettung und seit über 25 Jahren in der IT-Branche. Sein Expertenwissen umfasst Datenrettung im Storage-Umfeld (RAID 5, RAID 6), Herstellung virtueller Maschinen in unterschiedlichsten Umgebungen sowie Programmierung hauseigener Datenrettungssoftware und individueller Tools. Nicolas Ehrschwendner



Dipl. Ing. Nicolas Ehrschwendner, Gesellschafter, Attingo Datenrettung

1.2.2 Ansätze und Lösungen

Hackers Paradise – Sicherheit im Internet of Things

Im Zuge des digitalen Fortschritts stehen vor allem Chancen und praktische Features im Fokus. Was aber ist mit der Sicherheit? Wir vergessen gerne: Die bequemste Lösung ist nicht unbedingt auch die sicherste.

Dass die IT-Sicherheit im Kontext der Schlagworte Digitalisierung, Internet of Things (IoT) und Industrie 4.0 nicht immer den notwendigen Stellenwert genießt, ist nüchtern betrachtet kein neues Thema. Bereits 2010 zeigte sich, dass die Bedrohung mehr als nur theoretischer Natur ist: Die LNK-Lücke und der Stuxnet-Wurm legten Industrieanlagen in den USA, Südkorea, dem Iran und UK lahm. Einfallstor waren veraltete SCADA-Systeme (Computersysteme für das Steuern und Überwachen technischer Prozesse) bei denen versäumt wurde, entsprechende Sicherheitsmechanismen nachzurüsten. Ein düsteres, aber hochspannendes Bild eines solchen Angriffs zeichnete der Autor Marc Elsberg in seinem 2012 erschienenen Thriller „Blackout – Morgen ist es zu spät“: Ein Hackerangriff auf das Stromnetz schickt Europa zurück in die digitale Steinzeit. Waren Maschinensteuernetze in der Vergangenheit meist isoliert und nur durch menschliches Versagen oder Social Engineering zu knacken, sind wir im Zeitalter des IoT über Smart Homes (in direkt mit diesen Infrastrukturen verbunden) und die Anzahl der Angriffspunkte explodiert exponentiell. Und trotz allem waren in den letzten Jahren – scheinbar völlig befreit von derartigen Bedrohungsszenarien – unzählige Pilotprojekte im x-ten Sprint und es wurden fleißig Use Cases für das B2B- und B2C-Geschäft entwickelt, deren Früchte wir heute in unseren Smart Homes auskosten. Für den Laien war der Dschungel an Schlagworten bereits damals kaum durchschaubar und Aspekte der Sicherheit wurden somit weder hinterfragt noch von den Anbietern in den Fokus gerückt: Man musste ja erst einmal die Lösung an den Markt bringen – Hauptsache, man ist dabei.

Sicherheitslücken diskutiert und trotzdem ignoriert?

Gerade durch das Schaffen von schnellen, nahe liegenden Lösungen wurden signifikante Sicherheitsprobleme ignoriert. Vielleicht hat der eine oder andere Besitzer eines modernen Autos schon einmal darüber nachgedacht, ob die Nutzung von Apps der Automobilhersteller zum „Remote-Car-Ma-

agement“ wirklich sicher ist? Das Auto per App aufschließen: Eine tolle Sache, jedoch sollte man bedenken, dass der sogenannte CAN-Bus – die Daten-Aorta des Autos – aus den 80er-Jahren stammt und bei manchen Autos sogar über den Außenspiegel zugänglich ist. Fakt ist: Im schlimmsten Fall könnten über Schwachstellen im CAN-Bus komplette On-Board-Systeme deaktiviert werden. Dass es sich hierbei nicht um pure Theorie handelt, zeigen offizielle Warnungen des Industrial Control Systems Cyber Emergency Response Teams (ICS-CERT), das dem US-amerikanischen Department of Homeland Security untergeordnet ist.

2017 erreichte das Thema ein neues Level, als die US-amerikanische Lebens- und Arzneimittelbehörde FDA eine Sicherheitslücke in Herzschrittmachern identifizierte und tausende von Geräten aktualisiert werden mussten – alleine in Deutschland rund 13.000. Zwar war keine OP notwendig, aber ein persönliches Update beim Arzt. Man kann gespannt sein, was die nächste Stufe zu ambulanten Security Patches ist. Gut, wenn man als Arzt Informatik im Nebenfach studiert hat.

Die Liste an Sicherheitslücken ließe sich noch beliebig weiterführen. Hand aufs Herz: Sind sie sich dieser Punkte bewusst – als Fahrer eines modernen Autos, im Smart Home oder einfach nur als Fahrgast in einem durch IoT und künstliche Intelligenz überwachten Aufzug? Da erscheint es schon fast harmlos, wenn Amazons Alexa ohne Aufforderung Musik abspielt. Dumm nur, wenn das in der Nacht passiert, sie alleine Zuhause ist und die Polizei wegen Ruhestörung ausrückt. Besagter Fall ging Ende 2017 durch die Presse. Log-Analysen lassen vermuten, dass Alexa durch eine Spotify-Playlist ausgelöst wurde. Am Ende übernahm Amazon kulanterweise die Kosten für den Polizeieinsatz und ein neues Türschloss – das Szenario an sich sollte aber zum Nachdenken anregen.

Quo vadis Security?

Spricht man mit Anbietern von IoT-Plattformen sowie mit deren Leuchtturmkunden, hört man – wie nicht anders zu erwarten – ausnahmslos das Plädoyer: „Sicherheit steht an erster Stelle“. Das bestätigt auch die aktuelle IDG-Studie „Internet of Things 2018“. Hier werden Security und Datensicherheit als die größten Herausforderungen benannt. Dem gegenüber steht, gerade am B2C-Markt, ein zunehmender Preisdruck, der eine günstige Fertigung in verschiedensten Teilen der Welt erfordert. Dazu kommt, dass in der Studie zwar mehr als 50 Prozent Security-Technologien für unverzichtbar halten, sie jedoch nur rund 30 Prozent einsetzen. Der perfekte Nährboden für kuriose, bedenkliche oder auch gefährliche Sicherheitslücken.

Nur langsam wächst das Sicherheitsbewusst-

sein der Consumer und es wird ein verhaltener Ruf nach mehr Sicherheit laut. Zwar fangen Hersteller nach und nach an, ihre Cloud-Kommunikation zu verschlüsseln – aber wie können so viele Schlüssel sinnvoll gemanagt werden, wenn Geräte herstellübergreifend miteinander reden sollen? Stichwort exponentielles Wachstum. Und bei unsicheren Schlüsseln kann man auch gleich ganz auf Verschlüsselung verzichten.

Auch die Vielzahl an möglichen Protokollen macht es nicht einfacher, einheitliche und somit potenziell sichere Standards zu schaffen. Zu groß ist die Zahl an IoT-Plattformen bzw. derjenigen, welche sich als solche vermarkten. Natürlich wollen alle an dem gigantischen IoT-Markt mitverdienen. Wobei in den nächsten fünf Jahren durchaus eine erhebliche Konsolidierung bzw. Fokussierung zu erwarten ist.

Gibt es eine Lösung?

Persönlich hoffe ich auf die große Revolution des Internet of Things durch die Blockchain. Die Chancen sind hier sehr groß – solange das Konzept Blockchain sicher ist. Allerdings bedeutet dies einen deutlichen Wandel der IoT-Welt: Die Cloud muss dezentral werden, die Logik muss in die Geräte wandern, zentrale Steuerungssoftware verschwinden. Erst dann kommen wir tatsächlich zu einem Internet, in dem die Dinge miteinander reden und Akteure in Echtzeit Entscheidungen treffen und umsetzen.

Doch macht ein solcher Ansatz die IoT-Welt wirklich sicherer? Bezogen auf den technischen Aspekt vielleicht, aber wie gut können wir die Kommunikation der Dinge dann noch steuern und überwachen: Gerade, wenn neue Dimensionen wie künstliche Intelligenz mitmischen. Möchte man wirklich, dass die Waage mit dem Auto aushandelt, ob man heute besser zur Arbeit laufen sollte? Die Entwicklung bleibt spannend.

Jan Junker

IoT: Risikomanagement nur mit Security by Design

Das Internet der Dinge bildet den Kern aller Anstrengungen zur Digitalisierung der Industrie. Die beiden entscheidenden Wesensmerkmale sind dabei die Vernetzung von Maschinen und die Verarbeitung von Laufzeitdaten in Echtzeit in der Cloud. So werden Innovationen wie Predictive Maintenance oder Continuous Production Optimization möglich, die eine wesentliche Verbesserung der Produktivität bei gleichzeitig sinkendem Personalaufwand versprechen. Doch die Digitalisierung erhöht auch die Anforderungen an die IT-Infrastruktur, die durch die neuen Schnittstellen mit der Außenwelt potenziell verwundbarer wird. Bestehende IT-Infrastrukturen wurden oft nicht im Hinblick auf eine Erreichbarkeit vom Internet ausgelegt, und die bestehenden Sicherheitsmaßnahmen sind aufgrund widerstreben-



Jan Junker, Head of Business Unit Industries, PASS Consulting Group

der Anforderungen an die Ausfallsicherheit oft unzureichend. Spätestens mit der Vernetzung der Maschinen muss also mit einem aktiven Risikomanagement begonnen werden.

Risikomanagement und IT-Sicherheit

Ein bewährtes Mittel, um Risiken zu begegnen, sind Versicherungen. Cyberversicherungen werden mittlerweile von verschiedenen Anbietern angeboten. Allerdings sind das Leistungsportfolio und die maximalen abgedeckten Schadenssummen noch recht eingeschränkt. Folglich führt an Maßnahmen zur IT-Sicherheit kein Weg vorbei. Denn ein Verzicht auf technische Maßnahmen und eine ausschließliche Nutzung von Versicherungen würde zwangsläufig zu einem allgemeinen Anstieg an Sicherheitsvorfällen und somit Schadensfällen führen. Eine Versicherungspolice ist jedoch nur günstig, wenn die Anzahl der Schadensfälle gering ist. Steigt die Zahl der Sicherheitsvorfälle, wird auch die Cyberversicherung teurer. Cyberversicherungen sind somit allenfalls eine ergänzende Maßnahme auf dem Weg zur Industrie 4.0, können die eigentliche IT-Sicherheit aber nicht ersetzen. Immaterielle Schäden durch Cyber-Attacks wie belastete Kundenbeziehungen oder ein verschlechtertes Unternehmensimage – die oft schwerwiegender sind als die materiellen Einbußen – können mit Versicherungen zudem nicht oder nur unzureichend abgedeckt werden.

Cybersicherheit im IoT

Was also sind nun die größten Herausforderungen bezüglich der Sicherheit von industriellem IoT? Zunächst einmal die langen Investitionszyklen. So ist man sich unter Sicherheitsexperten weitgehend einig, dass eine Versorgung von Geräten mit aktuellen Sicherheitsupdates den höchsten Beitrag zur Sicherheit liefert. Die gelebte Praxis in vielen Unternehmen ist jedoch eine völlig andere. So werden nämlich bei laufenden Systeme keine Updates durchgeführt, obwohl Sicherheitslücken allgemein bekannt sind. Das liegt zum einen daran, dass viele Hersteller ihre Produkte nicht mit Updates versorgen. Aber auch die Sorge vor Störungen des Produktionsprozesses durch Updates ist groß, so dass diese gar nicht oder stark zeitverzögert eingespielt werden. An dieser Stelle können wiederum Versicherungen helfen, die Auswirkungen eines Produktionsausfalls im Zuge fehlerhafter Sicherheitsupdates zu minimieren.

Die zweite zentrale Herausforderung besteht darin, wie man Security by Design im IoT realisieren kann, um eine nachträgliche, teure Absicherung zu vermeiden. Der zur Zeit vielversprechendste Ansatz sind IoT-Plattformen, welche den IoT-Anwendungen eine sichere und dennoch funktionale Basis bieten

können. Datenbasierte IoT-Anwendungen bestehen typischerweise aus zwei Teilen. Zum einen werden die Maschinendaten bereits in den Produktionsanlagen vorverarbeitet und diese Zwischenergebnisse dann zur finalen Verarbeitung in die Cloud geschickt.

IoT-Gateway und Cloud-Gateway

Viele IoT-Plattformen folgen dieser Aufteilung in dem sie zwei Bestandteile zur Verfügung stellen: IoT-Gateways und das Cloud-Gateway. Die IoT-Gateways sind Geräte, die am Perimeter zwischen den Maschinen und dem Internet platziert werden. Sie stellen Basisfunktionen wie beispielsweise verschlüsselte Kommunikation oder sicheres Management zur Verfügung und bieten eine Laufzeitumgebung für IoT-Anwendungen, die eine Vorverarbeitung von Laufzeitdaten durchführen. Durch die strikte Trennung von Sicherheitssystemen und Anwendung kann ein hohes Maß an IT-Sicherheit bei größtmöglicher Flexibilität erreicht werden. Die Plattform bietet also Security by Design. Die eigentliche Datenverarbeitung führen die Anwendungen jedoch in der Cloud durch. Damit diese Daten dann vom zugehörigen IoT-Service in der Cloud verarbeitet werden können, werden sie verschlüsselt vom IoT-Gateway zu einem Cloud-Gateway geschickt.

Auch Anwendungen wie die sichere Fernwartung sind mittels IoT-Plattformen möglich. So kann ein Fernwartender sich mit einem Cloudservice verbinden, der wiederum mit einer korrespondierenden Fernwartungsanwendung auf dem IoT-Gateway kommuniziert. Die Durchsetzung der Sicherheit durch Verschlüsselung, Zugriffskontrolle und Monitoring wird durch die IoT-Plattform erbracht. Zugleich ermöglicht ihre Flexibilität ein Höchstmaß an Innovationsfähigkeit bei der Umsetzung neuer Anwendungen, welche die Industrie 4.0 ausmachen.

Fazit

Das IoT bietet die herausragende Chance, das Innovationspotenzial der Cloud in die Industrie zu tragen. Um den einhergehenden Risiken der Vernetzung zu begegnen, bieten sich Lösungen mit Security by Design als solide Basis und Cyberversicherungen als ergänzende Maßnahmen an.

Insbesondere sichere IoT-Plattformen haben das Potenzial, eine größtmögliche Flexibilität auf einem hohen Sicherheitsniveau zu erbringen. Claas Lorenz

Internet der Dinge: Security Guidelines

Internet of Things (IoT) und Smart Home sind spätestens seit Amazon Alexa in der Allgemeinheit angekommen. In Deutschland beträgt die Anzahl der Smart-Home-Haushalte etwa 750.000 [1]. Viele davon besitzen mehr als nur ein Smart-Home Gerät [2]. Im Jahr 2020 wird mit mindestens einer

Millionen Geräte gerechnet. Kein Wunder, helfen uns Smart-Home Geräte doch beim Energie sparen (Smarte Lampen/Steckdosen/Thermostate), sichern unser zu Hause (Smarte Türschlösser und Alarmanlagen, IP-Kameras, ...) und verbessern unsere Lebensqualität im Allgemeinen. Durch Assistenzsysteme wie Amazon Alexa können nicht nur Informationen per Sprachbefehl abgerufen werden, nein es lassen sich auch Smart Home Geräte damit steuern. Durch Technologien wie IFTTT (If this then that) können Geräte Aktionen ausführen wenn ein zuvor definiertes Ereignis auf einem anderen Geräte eintritt wie das Smart Lock wird entsperrt und es ist nach 18 Uhr, dann mache das Licht im Gang an. Kurzum: Internet of Things und Smart Home kann sehr praktisch sein und bietet viele Funktionen.

Allerdings kann diese Funktionsvielfalt auch missbraucht werden. Erfolgreiche Angriffe können teuer für die Opfer sein (Thermostat wird von einem Angreifer aus der Ferne aufgedreht, während die Bewohner im Urlaub sind), sie können gefährlich sein (Smarter Sauna-Ofen überhitzt), sie können unangenehm sein (Besitzer wird durch eigene IP-Kamera ausspioniert) oder alles zusammen: Eine per Smart-Lock verschlossene Tür wird geöffnet, um einzubrechen ohne dabei Spuren zu hinterlassen. Der Einbrecher kann viel stehlen (teuer), auf Privates stoßen (unangenehm) und Zeugen angreifen (gefährlich).

Sicherheit sollte also oberste Priorität haben. Die Wirklichkeit sieht bekanntlich anders aus, da sich Funktionen und Features besser verkaufen als Sicherheit. Insbesondere wenn Technologien noch recht neu sind, wird versucht, möglichst schnell ein Produkt auf den Markt zu bringen. Dies hat zur Folge, dass IT-Sicherheitsmaßnahmen bei Release des Produkts noch nicht hinreichend implementiert sind.

Allerdings hat sich das Sicherheitsniveau schon im Vergleich zu den Vorjahren erhöht – wenn auch nicht immer ausreichend. Das liegt mit daran, dass sich Standards wie ZigBee, Apple HomeKit oder Google Nest durchgesetzt haben und sich ein Trend zur Verlagerung in die Cloud erkennen lässt. Wobei letzteres zwar einen positiven Effekt für die sichere Umsetzung, jedoch negative Auswirkungen auf die Privatsphäre hat. Positiv ist die angestiegene Rechenkapazität der Prozessoren zu sehen, die (stärkere) Verschlüsselung unterstützen. Dennoch sind noch längst nicht alle Geräte sicher. Oftmals kann der Nutzer zwar unsichere Funktionen der Geräte deaktivieren (Zugriff aus dem Internet o.ä.), doch da längst nicht mehr nur technisch versierte Nutzer IoT-Geräte beschaffen, ist dies nicht ausreichend. Ein Gerät muss von Haus aus sicher sein und sicher bleiben. Hierzu sollten folgende sechs Prinzipien umgesetzt werden:

1. Automatische und sichere Firmware Updates
2. Zufällig generierte Passwörter statt Standardpasswörtern
3. Sichere Standardeinstellungen
4. Einsatz von Verschlüsselung
5. Datensparsamkeit (Datenschutz)
6. Bewährte Algorithmen verwenden

1 Automatische und sichere Firmware Updates

Seit 2016 befällt Mirai hunderttausende von IoT-Geräten wie IP-Kameras und fügt diese Geräte bereits existierenden Botnetzen hinzu [3]. Die ausgenutzten Sicherheitslücken sind bekannt und könnten geschlossen werden, doch für viele dieser Geräte ist gar kein Firmware-Update vorgesehen, weswegen Mirai wohl auch in den nächsten Jahren noch existieren dürfte.

IoT-Geräte sollten daher die Möglichkeit eines Firmware-Updates implementieren. Falls die Geräte Zugriff auf das Internet haben, sollte standardmäßig automatisch upgedatet werden. Doch neben automatischen Updates ist es auch wichtig, dass diese integer sind, korrekt eingespielt werden. Hat ein Angreifer die Möglichkeit die Firmware vor der Installation zu manipulieren, so wird durch das Firmware-Update ein neuer Angriffsvektor geschaffen. Für schnelle und sichere Firmware-Updates von IoT-Geräten gibt es mehrere Ansätze [4]:

- Schnorr-Updates
- PC-basiert
- Physical unclonable function (PUFs)
- Blockchain
- Schneider-IoT Update Mechanismus
- Mongoose OS

Jeder dieser Ansätze hat Vor- und Nachteile. Als Entwickler ist es daher empfehlenswert, diese Ansätze zu vergleichen, um die passende Lösung für die eigene Anwendungsumgebung zu finden.

2 Zufällig generierte Passwörter statt Standardpasswörtern

Viele IoT-Geräte besitzen Standardlogins wie admin:admin oder root:1234. Sind diese Geräte aus dem Internet aus erreichbar und ändert der Nutzer nicht das Passwort, so hat der Angreifer leichtes Spiel. Geräte mit Standard-Passwörtern sind schnell im Internet bekannt und durch Suchmaschinen wie Shodan für jedermann (!) leicht zu finden. Auch von fest enkodierten Service-Passwörtern ist abzurufen, da diese durch Reverse Engineering gefunden und dann ebenfalls ins Internet gestellt werden können. Besser wäre es so zu verfahren, wie es seit Jahren bei Routern üblich ist: Ein zufällig generiertes Passwort, welches dem Geräte durch beispielsweise einen Aufkleber beiliegt. Vergisst der Nutzer sein Passwort, so kann er durch Zurücksetzen des Gerätes den Urzustand wiederherstellen.



Claas Lorenz,
Researcher,
Genua GMBH



Wilfried Kirsch,
Security Consultant
softScheck GmbH
Sankt Augustin

3 Sichere Standardeinstellungen

Geräte sollten lieber mit zu sicheren als mit zu offenen Einstellungen ausgeliefert werden. Ein Thermostat oder eine IP-Kamera muss standardmäßig nicht aus dem Internet erreichbar sein. Ist dies dennoch erwünscht, so sollte der Nutzer dies manuell aktivieren können (Opt-In statt Opt-Out).

4 Einsatz von Verschlüsselung

Kommunikation zu Geräten und Servern sollte verschlüsselt stattfinden. Dies gilt vor allem dann, wenn die Geräte außerhalb des eigenen, verschlüsselten WLANs, per Funk miteinander kommunizieren. Ein Angreifer kann Daten-Pakete leicht abfangen, lesen oder gar verändern. Es sollte ein sicherer Algorithmus verwendet werden, der auch Modifikationen der Pakete erkennt.

5 Datensparsamkeit

Produkte sollten nur die nötigsten Daten versenden und speichern. Dies spart zum einen Ressourcen - vor allem aber limitiert es die Informationen, die ein Angreifer über das Opfer erfahren kann. Werden viele persönliche Daten versendet und gespeichert, sollte über eine Ende-zu-Ende Verschlüsselung nachgedacht werden.

6 Bewährte Algorithmen verwenden

Wenn es um IT-Sicherheit geht, sind ältere, bewährte Techniken oftmals besser als Eigenentwicklungen. Dies rührt daher, dass ältere Standards schon von vielen Personen getestet und für sicher befunden wurden. Natürlich bedeutet dies nicht, dass diese auch fehlerfrei sind (siehe Meltdown/Spectre). Eine Eigenentwicklung hingegen kann viele Fehler enthalten.

Fazit

Das Umsetzen dieser Punkte bietet keinen Garant dafür, dass das Produkt auch sicher ist. Es verringert allerdings die Angriffsfläche enorm. Soll das Produkt noch sicherer sein, bietet sich ein sicherer Entwicklungsprozess sowie das Testen von Produkten an. So basiert z.B. der softScheck Security Testing Process auf der ISO 27034 und enthält 6 Methoden zur Identifizierung von Sicherheitslücken: Security Requirements Analysis, Threat Modeling, Conformance Testing, Static Source Code Analysis, Penetration Testing und Dynamic Analysis: Fuzzing. Jeder dieser Methoden identifiziert andere Klassen von Sicherheitslücken. So konnten mit diesen Methoden schon Sicherheitslücken in Smart Meter Gateways und in der Smarten Steckdose TP-Link HS110 identifiziert werden. Wilfried Kirsch, Hartmut Pohl

Referenzen: [1] Statista (Hrsg.): Smart Home – Deutschland, <https://de.statista.com/outlook/279/137/smart-home/deutschland> [2] Connected Living (Hrsg.): Smart Home Index 2017, 2017, <http://www.connected-living.org/content/4-informati->

on/1-news/20171011-smart-home-index-2017-ist-smart-home-in-deutschen-haushalten-angekommen/20171004_sh_index_connected-living.pdf [3] D. Schirrmacher: Kriminelle bieten Mirai-Botnetz mit 400.000 IoT Geräten zur Miete an, 2016, <https://www.heise.de/security/meldung/Kriminelle-bieten-Mirai-Botnetz-mit-400-000-IoT-Geraeten-zur-Miete-an-3504584.html> [4] F. Barz: Sichere Firmware Over-The-Air Updates im Internet of Things, 2018

1.3 DIGITALE VERNETZUNG

1.3.1 Datenmanagement

Datenexplosion: wirtschaftliches Management und Hochverfügbarkeit dank Hyperscale-Rechenzentren

Das „Internet der Dinge“ ist in aller Munde. Dabei handelt es sich um eine wilde Ansammlung und Verschmelzung von Daten von allem, was Daten erzeugen kann und über eine Internetverbindung verfügt. Unabhängig von ihrer Größe benötigen IT-Abteilungen eine Strategie, um diese Daten zu erfassen, zu sichern und für ihr Unternehmen nutzbar zu machen. Tatsächlich werden nach einer Erhebung von Commvault nur rund 25 bis 30 Prozent der Daten in Unternehmen aktiv genutzt. Der Rest versteckt sich im Sekundärspeicher, beispielsweise in Form von Sicherungskopien, und ist schwer zugänglich.

Vertikale Skalierung (Scale-up) war lange Zeit der Branchenstandard im Zusammenhang mit Backup- und Recovery-Architektur für größere Datenmengen. Steigende Kosten und schlechte Auffindbarkeit sind gute Argumente, davon abzurücken. Denn niemand speichert Daten um des Aufbewahrens Willen. Anwender möchten sie abrufen können, und zwar schnell. In traditionellen Scale-up-Umgebungen kann der Datenzugriff sehr komplex und zeitaufwändig sein. Denn zuerst müssen Nutzer herausfinden, wo die Daten gespeichert sind – was mancherorts nahezu unmöglich ist. Dann müssen sie diese erst wiederherstellen. Dies kann Stunden oder sogar Tage dauern. Die meisten Anwender haben aber weder die Zeit noch die Geduld für einen derart langwierigen Prozess. Sie fordern immer häufiger eine gut funktionierende Self-Service-IT. Verantwortliche müssen Richtlinien anpassen, Rechte vergeben, Servicelevel sicherstellen... Das alles wird schnell zu einer zeit- und kostenintensiven Herausforderung.

Immer mehr führende Unternehmen befassen sich daher mit der horizontalen Skalierung (Scale-

out). Während der vertikalen Skalierung Grenzen gesetzt sind, da sich Rechner nicht endlos mit Hardware aufrüsten lassen, ist das Potential von horizontaler Skalierung schier unendlich, weil keine zusätzliche Appliances – externe Speichereinheiten aus Hard- und Software – nötig sind. Mit der passenden Scale-out-Technologie erhält man eine vollständige Hardware- und Softwarelösung in einem einzigen, benutzerfreundlichen Paket: Computing-, Speicher- und Netzwerk-Hardware sind dann nahtlos mit Datensicherungs-, Betriebssystem- und Virtualisierungs-Software integriert, so dass zahlreiche Kontaktpunkte zu einem einzigen reduziert werden. Dies minimiert Personal- und Verwaltungskosten, begrenzt übermäßiges Kopieren von Daten und vereinfacht die Anwendung von Richtlinien und Sicherheitskontrollen.

Skalierbarkeit ist nur von Vorteil, wenn die Nutzer auch einen webähnlichen Zugriff auf ihre Daten haben. Bei einem Scale-out-Ansatz bieten sekundäre Arbeitslasten ihren Nutzern und Anwendungen sofortigen Datenzugriff. Dies geschieht über eine Standardschnittstelle für alle verwalteten Daten, ob im Rechenzentrum oder in der Cloud. Selbst die anspruchsvollsten Anforderungen über mehrere Nutzer oder Anwendungen hinweg lassen sich unterstützen. So entsteht eine webähnliche Serviceverfügbarkeit. Durch die Verwendung integrierter Suchfunktionen können Anwender über Schlüsselwörter nach Dateien und Inhalten suchen – und neue Erkenntnisse schneller in Innovationen umsetzen.

Fazit

Die Digitalisierung durchdringt alle Branchen und Arbeitsbereiche, und das Datenvolumen steigt folglich ständig an. Die globalen Rechner- und Server-Infrastrukturen müssen mit dieser Entwicklung Schritt halten, und bislang gaben Internetgiganten wie Amazon, Facebook und Google dabei den Takt mit Hyperscale-Lösungen an. Unternehmen hatten anfangs Schwierigkeiten, Hyperscale in ihre Infrastruktur zu integrieren, jetzt kommt es aber auch im Mittelstand an. So stehen Unternehmen tatsächlich alle Daten zur Verfügung, wodurch sie Business-Intelligence-Lösungen bestmöglich für ihr Geschäft nutzen können.

Robert Romanski

Datenübertragung mittels Blockchain

Daten sind das digitale Gold. Es ist schon lange kein Geheimnis mehr, dass Google Millionen mit Benutzerdaten verdient. Facebook sammelte in zwei Wochen ein ca. 1.200 Seiten umfassendes PDF über den österreichischen Juristen und Datenschutzaktivisten Max Schrems[1] und verdient damit, wie mit jedem anderen Nutzer, fleißig Geld. Amazon kennt längst die Vorlieben seiner

Nutzer und schlägt „passende“ Produkte vor. Mittlerweile sitzt Amazon/Apple/Google auch mit Hilfe von Alexa/Siri/Google AI im digitalisierten Haushalt und bekommt so unendlich viele Daten. Diese digitalen Fußabdrücke, gespeichert in sog. Daten Silos, sind zwar meist „nur“ die Metadaten, doch lassen sich daraus Rückschlüsse auf private Daten (Arbeitszeiten, Konsumverhalten, Wohnort, ja sogar sexuelle Vorlieben etc.) des Nutzers schließen. Doch was hat das alles mit IoT zu tun?

Die Datenmenge, die Unternehmen zur Verfügung steht, wächst mit jedem IoT Device exponentiell! Jedes dieser Geräte unterstützt uns im Alltag, keine Frage, aber überträgt auch Daten zwischen Geräten. Genau diese Daten sind für Unternehmen sehr wertvoll. Eine eigene Infrastruktur für Daten zu bilden, ist sehr schwer, teuer und man stößt schnell an die Grenzen der Verarbeitungsgeschwindigkeit. Also greift man auf das zentrale System der Hersteller zurück.

Doch Systeme wie Alexa sind abhängig, wenn der Amazon Server ausfällt, geht nichts mehr. Und sollte Amazon keine Lust mehr am Geschäftsmodell haben - wird Alexa gar nicht mehr funktionieren, da kein Server mehr die Daten verwalten kann. Man spricht von einer zentralisierten Lösung.

Aber es gibt eigentlich gar keinen Grund für IoT Devices überhaupt mit einem Server als Schnittstelle zu arbeiten. Die meisten Informationen können direkt ausgetauscht werden.

Hier bietet die Blockchain und ihre „Geschwister“ eine interessante Alternative. Dies haben bereits einige, unter anderem deutsche Entwickler erkannt und entwickeln verschiedene Technologien, um es zu erschweren, Daten abzugreifen und/oder die Kommunikation zwischen den Devices sicher und schnell zu gestalten. Nun hat wie immer jede Technologie Vor- und Nachteile. Ein weiterer Vorteil der Blockchain als Kommunikationsmittel zwischen den Devices ist die Möglichkeit, den Zahlungsverkehr schnell, sicher und automatisiert abzuwickeln.

Blockchain - Basics

Um wirklich das Konzept hinter den Technologien zu verstehen, muss erst einmal verstanden werden, wie eine Blockchain funktioniert. Daher hier ein kurzer Abriss:

- Eine Blockchain besteht aus vielen Daten Blöcken, die aneinander gereiht werden:
 - o Jeder Datenblock bekommt via SHA256 einen individuellen Hash, der nicht rückwärts berechenbar ist.
 - o Der Hash des Vorblocks befindet sich in der Datenmenge des aktuellen Blocks.
 - o Da ein Hash derzeit nicht „fälschbar“ ist, zerfällt die Blockchain, sobald die Daten eines Blocks geändert werden

- Die Blockchain wird auf sehr vielen Rechnern (sog. Nodes) weltweit gespeichert und es herrscht Konsensus, die Mehrheit entscheidet was richtig ist:
 - o Falls ein Node gefälschte Daten einspeisen möchte, fällt allen anderen auf, dass diese Daten falsch sind und schließen ihn aus dem Netzwerk aus, bis die Daten wieder korrekt sind
- Man kann Daten durch einen Privat Key in die Blockchain einspeisen (Identitätsnachweis)
- Der Privat Key ist auf der Blockchain nicht sichtbar, sondern die Adresse des sogenannten Public Keys
- Ein Private Key kann mehrere Public Keys erzeugen, dies führt zu Anonymität
- Pro Überweisung/Datenübermittlung (im folgenden Tx genannt) entsteht eine kleine Gebühr

Das Konzept kann hier ausprobiert werden. Eine klassische Blockchain ist jedoch schnell im Datendurchsatz begrenzt. Der Bitcoin schafft lediglich ca. 13 Transaktionen/s zu verarbeiten, was bei der zu erwartenden Menge an IoT Devices lächerlich wenig ist. Hier kommen die alternativen Technologien zum Tragen.

Tangle/IOTA

Der Tangle ist eine Deutsche Erfindung und wird von der IOTA Foundation aus Berlin entwickelt. IOTA ist derzeit das größte IoT – Blockchain Projekt. IOTA ist eine sogenannte Kryptowährung, wird in Millionen als Einheit gehandelt und kostet derzeit ca. 2€. Das Geniale an dieser Technologie ist, dass die Geschwindigkeit der Datenübermittlung steigt, je mehr Daten übermittelt werden. Dies entsteht durch den Tangle. Während bei einer klassischen Blockchain alle Nodes im Netzwerk die Transaktionen in jedem Block bestätigen, geschieht dies im IOTA Netzwerk durch die Transaktionen selbst. Dadurch sind diese auch kostenlos. Jede neue Transaktion bestätigt zwei alte, nicht bestätigte Transaktionen. Es gibt in diesem Netzwerk keine Blöcke mehr, da der Konsensus durch den Tangle automatisch entsteht. In festgelegten Intervallen wird der entstandene Transaktionen-Baum gespeichert und eine neue Genesis-Transaktion erstellt, anhand derer ein neuer Tangle entsteht. Diese Technologie befindet sich derzeit noch in einer Beta Phase und hat viele Schwächen. Jedoch haben schon große Dax Unternehmen wie Bosch und VW bestätigt, an dieser Technologie zu forschen.

Die Idee von IOTA ist, dass nun jedes Device einen eigenen IOTA Privat Key hat und sich die Devices einzelne IOTA mit Befehlen zusenden können. Ein IOTA ist so günstig, dass die Kosten

nicht ins Gewicht fallen und durch die kostenlose Transaktion „verliert“ man auch kein Geld. Bei jeder Transaktion kann eine neue Adresse verwendet werden, somit ist es auch nicht möglich, Metadaten einzelner Geräte zu speichern. Tatsächlich setzt VW sehr große Hoffnungen in diese Technologie in Verbindung mit automatisiertem Fahren etc.. Daher hat Volkswagen den CDO Johann Jungwirth auch als neues Aufsichtsrats Mitglied und Berater in der IOTA Foundation eingesetzt.

Nano, ehemalig RailBlocks

Diese Technologie ist im Vergleich zu IOTA noch sehr jung und setzt auf die klassische Blockchain. Jedoch bekommt jeder Privat Key seine eigene Blockchain. Dadurch entsteht eine Gitterstruktur aus Blöcken. Eine Transaktion besteht aus zwei Blöcken. Einem Block auf der Sender- und einen auf der Empfänger-Chain. Dadurch muss das Netzwerk nur minimal Daten selber verarbeiten. Transaktionen sind auch bei dieser Technologie kostenlos. Um zu vermeiden, dass das Netzwerk mit Transaktionen zugespammt wird, haben die Entwickler, wie beim Bitcoin, einen Proof of Work Algorithmus eingebaut. Der Empfänger und Sender muss einen Arbeitsnachweis erbringen, um die Transaktion zu empfangen. Dies könnte jedoch auch zu einem großen Problem im IoT Bereich werden, da viele IoT Devices aus Kostengründen zurecht keine starke Rechenpower besitzen. Da die Technologie noch sehr jung ist, hat sie noch keine Anwendungsfälle oder Firmen, die offiziell eine Unterstützung angekündigt haben. Derzeit sind ca. 7.000 Transaktionen/s möglich, was ca. das 1000 fache gegenüber den klassischen Blockchains ist.

Hdac (Hyundai Digital Asset Currency)

Ist eine Technologie, die von Hyundai entwickelt und bereitgestellt wird. Hdac möchte ein ernstzunehmender Konkurrent zu IOTA sein und spezialisiert sich auf SmartHomes und SmartCars. Die Hdac Chain will es ermöglichen, einen eigenen Coin mittels Smart Contract zu kreieren (ähnlich wie bei Ethereum). Der größte Vorteil von Hdac gegenüber IOTA oder anderen Lösungen ist, dass sie eine private Blockchain ermöglichen. Somit sollten die SmartHome Devices nur in der eigenen Blockchain kommunizieren können. Dies führt zu einer sehr großen Sicherheit der Daten. Hdac ist jedoch eine der jüngsten Technologien unter den IoT Technologien und muss sich erst noch gegenüber IOTA und anderen behaupten, um sich am Markt zu platzieren. Getestet wurde die Blockchain bis jetzt mit ca. 150 Transaktionen/s auf der öffentlichen und 500 Transaktionen/s auf der privaten Blockchain. Das angestreb-

te Ziel von ca. 1000 Transaktionen/s ist derzeit noch nicht erreicht.

Wichtig für eine Technologie ist vor allem die Menge der Daten, die übertragen werden kann. Vermutlich werden die von Hdac angegebenen 1000 Transaktionen/s und auch die 7000 Transaktionen/s von Naon nicht ausreichen, sollte der IoT Markt sich wie erwartet entwickeln.

Alles im allen ist jedoch klar, dass noch keine der Technologien ausgereift ist. Potential ist trotzdem auf jeden Fall für alle vorhanden, eine richtige Anwendung wurde aber für noch keine dieser Technologien geschaffen. Da das Internet of Things ebenfalls noch in den Kinderschuhen steckt, bleibt zu hoffen, dass sich diese Technologien parallel entwickeln und immer ausgereifere Lösungen anbieten. Gerade IOTA ist dank der „unendlichen“ Skalierbarkeit sehr vielversprechend als Grundlage für den Daten- und Geldtransfer zwischen Devices.

Auch könnte Deutschland die verschlafene Technologiewende aufholen und sich dank IOTA stark im Bereich IoT positionieren. Leider gibt es bis dato noch keine Aussagen der Bundesregierung über mögliche und notwendige Regulierungen des „Neulands“ Blockchain, es wird also spannend bleiben, wie sich diese Technologie in den betrieblichen und privaten Alltag eingliedern wird.

Carsten Hochschon

Referenzen: [1] Bähr, Julia (2015, 23. September) FAZ URL: <http://www.faz.net/aktuell/feuilleton/medien/max-schrems-jahrelanger-kampf-gegen-facebook-13819522.html> [01.02.2018]

1.3.2 Auswirkungen

Vernetzt denken und handeln

Durchgängige Digitalisierung sowohl in den Produkten als auch in der Produktentstehung ist ein wichtiges Trendthema. Überall schießen Konzepte, Software und Tools zum Thema Industrie 4.0 aus dem Boden, die Vorteile durch digital vernetzte Systeme und Prozesse aufzeigen. Eine IDC Studie zum Thema Internet of Things stellt die Prognose auf, dass die Anzahl der vernetzten Dinge von weltweit aktuell 12,1 Mrd. bis zum Jahr 2020 auf 30,3 Mrd. ansteigen wird.

Doch der Knackpunkt für eine vollständig digitalisierte Entwicklung und Produktion liegt in einer ganzheitlichen Sicht aller Beteiligten auf sämtliche Vorgänge und Planungen entlang des gesamten Produktentstehungsprozesses. Konstrukteure müssen sich mit Nicht-CAD-Spezialisten austauschen können, verschiedene Disziplinen wie Mechanik, Elektrik/Elektronik und Software zusammenwachsen, Daten überall verfügbar sein. Aber auch bisher kaum integrierte Fachberei-

che wie psychophysiologische Wissenschaften, Neurobiologie oder Rechts- und Wirtschaftswissenschaften sollten im Sinne einer ganzheitlichen Produktentwicklung berücksichtigt werden. Seit einigen Jahren wird Systems Engineering als vielversprechender Ansatz dafür in der Fachwelt diskutiert und auch angewendet.

Immerhin war eines der prominentesten Anwendungsgebiete die technische Planung und Umsetzung der Mondlandung. Die Anforderungen bei diesem Projekt waren unklar, die Umgebung unbekannt. Doch um mögliche Risiken zu reduzieren, bedarf es der Spezifikation von operativen Konzepten bis hin zu technischen Lösungen. Hier bietet Systems Engineering Lösungsansätze – damals wie heute.

Das Interesse am Thema ist riesig. Die Mitgliedszahlen bei der Deutschen Gesellschaft für Systems Engineering (GfSE) steigen. Offenheit und Transparenz sind in aller Munde, aus zwei Gründen: Man hofft auf sinkende Kosten, verbesserte Produktqualität und mehr Planungssicherheit. Zudem versprechen sich die Beteiligten von einem modellbasierten Entwicklungsansatz einen besseren Umgang mit den steigenden komplexen Anforderungen.

Komplexe technische Systeme wie das autonome Fahren, die Elektrifizierung im Antriebstrang von Autos oder die Vernetzung von Maschinen und Anlagen steigern die Komplexität von Produktentwicklungsprozessen in einer bisher nicht da gewesenen Weise. Gleichzeitig verändern sich auch die rechtlichen Rahmenbedingungen. Umfassende Nachweispflichten zur Durchgängigkeit von Entwicklungsprozessen sowie die Rückverfolgbarkeit des kompletten Produktentstehungsprozesses (Traceability) werden zunehmend von Kunden und Behörden im Rahmen der Produkthaftung eingefordert.

Nur ein ganzheitlicher Ansatz bei der Entwicklung von Produkten schafft die notwendige Transparenz für alle beteiligten Gruppen. Systems Engineering spannt im Sinne des Product Lifecycle Managements (PLM) den Bogen von der Anforderungsermittlung über die technische Implementierung und das fertige Produkt bis hin zum Recycling.

Die Aufgaben sind vielfältig und interdisziplinär. Sie umfassen Systemanalyse, Anforderungsermittlung, Systementwicklung, Absicherung und Testphase. Ziel ist es, die zahlreichen Funktionen unterschiedlicher Disziplinen in einem komplexen System möglichst modellbasiert zu beschreiben und mit vielen integrierten Projektbeteiligten auf nur einer Plattform zeitgleich zu bearbeiten. Um dabei einen reibungslosen Ablauf zu gewährleisten, ist es notwendig, den Entwicklungsprozess



Dr.-Ing. Darko Sucic
Senior Director und
Leiter des Center of
Excellence „Digital
Manufacturing“,
Dassault Systèmes



Carsten Hochschon,
CEO, Geschäftsführer
und Gründer,
knoing GmbH

vollständig zu digitalisieren und gleichzeitig die Entwicklungsdaten zu vereinheitlichen.

Die heute noch überwiegend dokumentenzentrierte Systementwicklung mittels Lastenheft, das Tausende von Anforderungen beinhaltet, hin zu einem datenbankgestützten Requirements-Engineering-Werkzeug lässt sich durch die modellbasierte Entwicklungsmethodik MBSE erheblich verbessern. Sie beschreibt alle Anforderungen und Spezifikationen für das spätere Produkt und koordiniert dessen gesamten Lebenszyklus, einschließlich der Qualitätstests und der Anforderungen an das spätere Recycling.

Modellbasiert bedeutet auch, dass es nur noch eine digitale Repräsentanz des Projektes gibt, an der alle Beteiligten z.B. in einem global verteilten Entwicklungsprozess arbeiten. Dadurch entsteht automatisch die notwendige Kollaboration und Vernetzung zwischen den interdisziplinären Teams innerhalb des digitalisierten Produktentstehungsprozesses. Jede einzelne Änderung ist auf der Arbeitsplattform sofort für alle sichtbar. Es steht immer nur eine aktuelle Version zur Verfügung (Single Source of Truth). So lassen sich Fehler vermeiden sowie Zeit und Kosten sparen. MBSE bildet das jeweilige System einschließlich seiner Sub-Systeme komplett ab und erlaubt zudem dessen Bewertung. Die Entwickler leiten aus den Kundenanforderungen die notwendigen Prozesse und Werkzeuge ab und beschreiben diese mithilfe verschiedener Modelle nachvollziehbar. Ein kritischer Erfolgsfaktor liegt in der Durchgängigkeit der Daten oder der Wiederholbarkeit der Prozesse. Dabei bindet MBSE die jeweils vorhandenen Modelle des Systems über geeignete Schnittstellen ein. Um das Systemmodell zu erstellen, gibt es unterschiedliche Sprachen wie zum Beispiel SysML, Methoden und IT-Werkzeuge. Sie lassen sich auch verschieden miteinander kombinieren. Allerdings fehlen hier noch vereinheitlichte Methoden und Standardschnittstellen.

Die große Herausforderung für Unternehmen besteht deshalb darin, ihre PLM- oder MBSE-Konzepte in der Zukunft miteinander zu verbinden. Die Einführung eines integrierten Systems wie der 3DEXPERIENCE Plattform von Dassault Systèmes, in der alle Autorentsysteme in einer zentralen Datenbank miteinander verknüpft werden, gilt als nachhaltiger und unvermeidlicher Lösungsansatz.

Die modellbasierte Systementwicklung erfordert aber nicht nur neue Werkzeuge und Standards. Sie verlangt auch ein anderes Denken, organisatorische, prozessuale und methodische Veränderungen in den Unternehmen. Die einzelnen Mitarbeiter der verschiedenen Fachbereiche müssen frühzeitig integriert werden – mit dem

Ziel, eine gemeinsame Herangehensweise verbunden mit einheitlicher Systembeschreibung und Systemdenken zu entwickeln. Die große Herausforderung lautet: Den Dialog mit den beteiligten Menschen führen, sie abholen und für das Thema begeistern, weil sie die Vorteile überzeugen. Denn Systems Engineering ist zweifelsfrei sinnvoll für die anstehenden Aufgaben. Dr.-Ing. Darko Susic

Ein neues Netz als Herzstück für intelligente Städte

Wo Digitalisierung und Glasfaser in aller Munde sind, bietet das Internet der Dinge Großkonzernen und Mittelständlern die Möglichkeit, sich als industrielle Vorreiter frühzeitig Wettbewerbsvorteile zu verschaffen. Längst können aber auch Städte und Kommunen von digitalen Lösungen profitieren. Führende Lokalpolitiker setzen zunehmend auf die Positionierung der eigenen Stadt als „Smart City“. Das steigert das Image. Vor allem aber profitieren davon die Bewohner tagtäglich. Beispielsweise wenn Innenstädte oder Bahnhöfe dank vernetzter Mülleimer sauberer bleiben. Und sie profitieren davon auch langfristig und indirekt. Denn wenn die städtischen Stromkosten durch intelligente Beleuchtungssysteme reduziert werden, können die zusätzlichen finanziellen Mittel anderweitig genutzt werden. Kultur- und Freizeitangebote der Stadt können so beispielsweise wieder verstärkt in den Fokus rücken.

Narrowband IoT – ein Netz für Maschinen macht Städte smart

Sprechende Mülleimer, die der Stadtverwaltung automatisch melden, wenn Sie geleert werden müssen oder intelligenten Straßenlaternen, die nicht mehr unnötig Strom verbrauchen, sind erst der Anfang der digitalen Möglichkeiten für Städte und Kommunen. Mit dem Internet der Dinge lässt sich die gesamte innerstädtische Infrastruktur optimieren. Die Anwendungsszenarien sind nahezu grenzenlos. Das gilt für Großstädte ebenso wie für kleinere Kommunen. Das Herzstück für die Vernetzung von Städten wird das neue Maschinen-Netz (Narrowband IoT), das Vodafone jetzt über Deutschland legt. Es ist speziell für die Vernetzung von Gegenständen optimiert. Millionen Mülleimer, Straßenlaternen, Alarm- und Überwachungssysteme oder Strom- und Wasserzähler können so gleichzeitig und kostengünstig vernetzt werden. Und das sogar an Orten, an denen Mobilfunk sonst nur schwer hinkommt – hinter massiven Hauswänden oder tief unter der Erde. Eine externe Stromversorgung benötigen Narrowband IoT Sensoren, die beispielsweise aktuelle Füllstände, Temperaturen oder Feuchtig-

keit erkennen nicht. Akkulaufzeiten von bis zu 10 Jahren machen sie unabhängig von der Steckdose.

Intelligente Straßenbeleuchtungen und sprechende Mülltonnen

Mit diesen Eigenschaften wird das Maschinen-Netz in Zukunft die Infrastruktur für Smart Cities. Bewohner der Innenstädte und Ihre Besucher beispielsweise können von intelligenten Parkleitsystemen profitieren. Spezielle Narrowband IoT Sensoren unter der Erde oder an Straßenlaternen würden dann ständig feststellen, welche Parkplätze belegt sind und an welchen Orten noch freie Kapazitäten für Fahrzeuge existieren. Dafür benötigt es innerstädtisch tausende Sensoren, die die Daten regelmäßig und verlässlich an die Smartphones der Autofahrer übertragen. Eine kostengünstige und robuste Datenübertragung ist dafür elementar. Mit Narrowband IoT Sensoren ausgestattete Straßenlaternen könnten zudem genau erkennen, wann eine Straßenbeleuchtung benötigt wird und diese optimal an die Außenbedingungen anpassen. Das birgt enormes Einsparungspotenzial. Einsparungen, die an anderer Stelle sinnvoll investiert werden können, um die Attraktivität eines lokalen Wirtschafts- und Kulturstandortes weiter zu steigern.

Auch der gesamte Prozess der Stadtreinigung könnte ins Internet der Dinge wandern. Öffentliche Mülltonnen würden der Stadtverwaltung dann über das Maschinennetz melden, wann sie geleert werden müssen, um nicht überzulaufen. Aus der Zentrale heraus könnten so automatisch die Routen der Einsatzfahrzeuge optimiert werden. Weiter gedacht können davon auch private Haushalte profitieren. Die Müllabfuhr müsste dann nicht mehr in jede Tonne schauen, um zu sehen, ob diese geleert werden muss. Das macht die Arbeit der städtischen Müllabfuhr effizienter und den Alltag für die Bewohner einfacher.

Im Alltag würden sich in smarten Städten auch digitale Strom- und Wasserzähler bemerkbar machen. Das Warten auf den Ausleser hätte damit ein Ende. Stromzähler können über das Maschinennetz sogar aus tiefen Kellern aktuelle Zählerstände übermitteln. Stündlich, täglich, wöchentlich. Genau in der Taktung wie vom Versorger oder Nutzer gewollt. Fehler bei der Auslesung und dadurch entstehende Mehrkosten würde das ausschließen. Das freut den Verbraucher.

Grenzenlose Möglichkeiten für die Vernetzung in Städten

Und die Möglichkeiten der Vernetzung in Städten gehen weiter: Überlegungen reichen von Haltestellen, die Busfahrern automatisch melden, ob Fahrgäste an der Haltestelle warten und ob diese

deshalb angefahren werden muss, bis zu digitalen Alarmanlagen gegen illegale Graffiti – beispielsweise an historischen Stadtmauern. Dazu hat Vodafone gemeinsam mit Studenten sogar schon einen ersten Prototypen entwickelt. Dieser enthält drei Sensoren. Sie erkennen Bewegung, Farbpartikel und typische in Graffiti-Farbe enthaltene Gase. Schlagen alle drei Sensoren aus, könnte über das Maschinennetz ein Alarm ausgelöst werden. Entweder direkt vor Ort zur Abschreckung der illegalen Sprayer. Oder ein „stiller Alarm“ geht in einer Zentrale ein, die dann Sicherheitskräfte zum jeweiligen Tatort aussendet.

Die Breite der Beispiele zeigt: Hinter der „smart city“ steckt deutlich mehr, als ein positiver Imageeffekt. Viel mehr kann das Internet der Dinge Städten und städtischen Unternehmen die Arbeit erleichtern und Bewohner im Alltag unterstützen. Das stärkt in der Folge das gesamte Stadtbild und fördert die städtische Entwicklung ebenso wie den regionalen Tourismus. Jochen Busch

Das Internet wird unsichtbar

E-Commerce in der IoT-Welt

Die Wahrnehmung des Internets und die Art damit zu interagieren, wird sich in der Welt des Internet of Things (IoT) maßgeblich verändern. Seit dem Start der ersten Internetdienste wurde dessen Nutzung mit Computern und Monitoren assoziiert. Der erste große Wandel erfolgte durch den hinlänglich bekannten Durchbruch der Smartphones, allen voran des iPhones im Jahr 2007. Dadurch wurde das Internet zum Alltagsbegleiter in der Hosentasche und gewann insbesondere an Mobilität, war aber gleichzeitig noch hochgradig auf die Nutzung durch einen Screen ausgerichtet.

Aktuell erleben wir nun den dritten großen Entwicklungsschritt in der Onlinewelt: Das Internet weitet sich auf Gegenstände aus, die keinen Bildschirm mehr besitzen und auf den ersten Blick teilweise auch gar nicht den Anschein erwecken, überhaupt „online“ zu sein oder gar eine elektrische Komponente zu enthalten.

Wie schon bei vielen Technologien zuvor zu beobachten, ist auch diese Entwicklung im industriellen Umfeld bereits länger sichtbar - und zwar insbesondere in Form von Sensorik, die dazu genutzt wird, fortlaufend Daten zu erfassen, um Prozesse zu überwachen und zu steuern.

Neu ist die rasant zunehmende Durchdringung von mit dem Internet verbundenen Alltagsgegenständen bei Endkunden in deren eigenen vier Wänden. Neben den gewohnten digitalen Geräten, wie dem Laptop, dem Smartphone oder dem Fernseher findet sich Internet-Konnektivität inzwischen bereits im Babyphone, der Waschmaschine oder der Zahnbürs-



Jochen Busch,
Head of IoT
Central Europe,
Vodafone GmbH



Florian Hermsdorf,
Head of Innovation
Management der
Otto Group

te. Daran wird langsam deutlich, wie unsichtbar und allgegenwärtig das Internet für alle werden wird.

So verwundert es auch kaum, dass aktuelle Erhebungen, unter anderem von Gartner, zeigen, dass es weltweit bereits über acht Milliarden vernetzte Geräte gibt und die Anzahl bis 2020 auf über zwanzig Milliarden steigen soll. Dies bedeutet, dass wir aktuell nur auf den Anfang einer fundamentalen Veränderung unserer Onlinenutzung blicken, bisher lediglich die sprichwörtliche Spitze des Eisbergs sehen können. Das Internet wird zunehmend unsichtbar und gleichzeitig allgegenwärtig, wie elektrischer Strom.

IoT als Grundlage für antizipative und automatisierte Handlungen

Die bisherige Onlinenutzung, wie zum Beispiel eine Websuche, Musikstreaming oder ein Onlinekauf, sind jeweils geprägt von einem starken Nutzer-Engagement. Das bedeutet, dass der Nutzer zum einen überhaupt aktiv werden muss und zum anderen seinen Wunsch möglichst konkret durch Nutzung zum Beispiel einer Sucheingabe ausformuliert. Entsprechend können diese Aktivitäten gerade in Situationen frustrierend werden, in denen der Bedarf sehr offensichtlich ist (Der Kühlschrank ist leer) oder der Wunsch nur ungenau geäußert werden kann („Entspannte Musik abspielen“).

Wenn nun mittels „Internet of Things“ zahlreiche neue Sensoren im Alltag des Nutzers dazukommen und diese laufend das Umfeld und die aktuelle Situation analysieren, können auch Nutzerbedürfnisse weitaus vorausschauender abgeleitet und darauf basierend sogar proaktiv erfüllt werden. So müssen Nutzer offensichtliche Wünsche nicht mehr benennen und können darauf vertrauen, dass ihr IoT-befähigtes, smartes Zuhause viele Dinge selbständig erledigt - wie zum Beispiel das Licht automatisch mit der passenden Helligkeit einzuschalten, sobald man die Wohnung betritt, oder die passende Musikauswahl über einen Smart-Speaker zu spielen.

E-Commerce in der IoT-Welt

Es ist auch davon auszugehen, dass diese IoT-geprägte Welt einen wesentlichen Einfluss auf das bisherige Onlineverhalten haben wird. Der Onlinezugang über Geräte mit Displays wird nicht wegfallen, allerdings in der Relevanz der gesamten Internet-Nutzungszeit geringer werden. Nutzer werden sich voraussichtlich zunehmend daran gewöhnen, dass ihre Bedürfnisse frühzeitig antizipiert und bestimmte Dinge im Hintergrund unkompliziert direkt für sie erledigt werden, ohne dass es noch einer weiteren Handlung ihrer selbst bedarf.

Die Omnipräsenz des Internets in Alltagsgegenständen wird schlussendlich auch zu einer Veränderung des Kaufverhaltens führen. So ist denkbar, dass der Vorratsschrank ohne manuelles Zutun immer ausreichend gefüllt ist, weil der Bestand der Lebensmittel fortlaufend überwacht und notwendige Nachbestellungen automatisch angestoßen werden.

Für E-Commerce Unternehmen stellt sich daher die Herausforderung auch auf den neuen Touchpoints kundenrelevant vertreten zu sein. Hierzu wird es nicht mehr ausreichen, einen performanten und nutzerfreundlichen Webshop zu haben, da Online-Nutzer sich nicht mehr nur in der ehemaligen Webwelt aufhalten werden. Die Services und Angebote müssen entsprechend IoT-fähig werden, um auch in einer „No-Screen“-Welt genutzt werden.

Bei der Otto Group wissen wir sehr genau um diese Herausforderungen und haben deshalb schon vor längerer Zeit ein Team zusammengestellt, das sich ganz konkret mit diesen Themen beschäftigt und Lösungsansätze erarbeitet. Ein zwingend notwendiger Schritt für Handelsunternehmen, die auch in Zukunft – anders als das Internet – sichtbar bleiben wollen.

Florian Hermsdorf

(di)IoT – wie Smart Devices unserer Gesellschaft Innovation vorgaukeln und unseren Alltag komplexer machen

Das Internet der Dinge (Internet of Things – kurz IoT) ist keineswegs eine wirklich neue Erfindung in der IT-Industrie. Bereits in den späten 80ern und frühen 90ern kam erstmals eine Vision von einer durch Technologie stark geprägten Welt auf. „Ubiquitous Computing“ (kurz und äquivalent unsexy UbiComp) nannte Mark Weiser die Idee, die er am Xerox PARC Forschungszentrum mitentwickelte. Eine Idee von einer Welt, in der es keine einzelnen, großen Computer mehr gibt, sondern in der wir permanent von rechnenden Maschinen umgeben sind, die sich elegant in unsere Umwelt integrieren. Allgegenwärtige Rechner, die sich natürlich anfühlen und praktisch unsichtbar für uns Menschen sind, weil es keine einfachen Maschinen mehr sind, sondern gänzlich neue, innovative Dinge, in denen Technologie auf intuitive Art und Weise verwoben ist.

Heute blicken wir auf eine ganze Palette von Smart Devices, die sich unter dem Oberbegriff des Internet der Dinge tummeln. Kühlschränke mit Kameras und Bluetooth, Thermostate mit Sprachsteuerung, Waschmaschinen mit WLAN, Elektrozapfsäulen mit RFID-Schnittstelle, SmartTVs, Smartphones, Smartwatches. Das IoT wird gerne als „smart“ ausgelegt, dabei stellen sich viele dieser Technologien als weitaus dümmer heraus, als die ursprünglichen Dinge, die es noch vor wenigen Jahren ohne Internetanschluss gab, was vor allem an den

eigentlichen Herstellern liegt. Sicherheitsstandards werden in manchen Fällen gerade zu spektakulär missachtet, an jeder Ecke werden Daten erhoben und übers Internet an den Hersteller zur Verarbeitung verschickt, und dann am besten gleich noch in einer Cloud hochgeladen und auf einer freshen Benutzeroberfläche mit Material Design dem Nutzer präsentiert, als wäre der Technologiegigant im Hintergrund der Retter des menschlichen Wohlbefindens.

Doch schieben wir für einen Momentan die kritischen Bedenken zur Seite und schauen unvoreingenommen auf die Errungenschaften der IoT-Industrie, so bleibt dennoch die große Freude meist auf der Strecke. Als spiritueller Nachfolger zur Vision des UbiComp entpuppt sich das Internet of Things als plakative Technologisierung von alltäglichen Dingen, die all ihre Probleme bereits teilweise vor Jahrzehnten genau so gut lösten, wie sie es heute tun. Eine Waschmaschine mit WLAN wäscht auch heute noch nach dem selben Prinzip wie vor 20 Jahren. Sie mag inzwischen weniger Wasser und Energie verbrauchen (und das ganz ohne Internetanbindung), aber die eigentliche Funktion ist erhalten geblieben. Doch offenbar ist es in der modernen Welt des IoT wichtig, dass Spülprogramme über eine unhandliche App auswählbar sind, für die ich mich beim Hersteller mit einem extra Konto registrieren muss. Da kann ich dann auch live verfolgen, wie der Waschgang fortschreitet. Ich könnte sie auch so programmieren, dass sie zu einer bestimmten Zeit fertig ist. Die Wäsche muss ich natürlich trotzdem per Hand einfüllen, ich stehe also doch irgendwann vor meiner Maschine und kann gleich da alles einstellen. Alles, was die App in diesem Fall macht, ist, mir die bereits bestehenden Funktionen und Informationen über das Internet bereitzustellen. Keine Innovation, keine Revolution, nur eine andere Lösung für ein Problem, das bereits gelöst wurde.

Und dabei stellt sich häufig die technologisierte Lösung als die deutlich aufwendigere heraus. Ein Thermostat mit Sprachsteuerung ist kein besserer Thermostat. Wenn ich in meiner Wohnung die Heizung anschalten möchte, reicht eine Drehung an einem kleinen Kasten an der Wand. Ein Handgriff, intuitiv und für praktisch jeden Menschen nachvollziehbar. Doch schaltet sich Alexa zwischen mich und meine Heizung, so muss ich nicht nur die richtigen Worte wählen, sondern auch auf meine Artikulation achten. Und ich will gar nicht erst darüber nachdenken, was wohl passiert, wenn ich die Heizung mal auf Englisch anschalten möchte.

Irgendwie haben es Gerätehersteller geschafft uns Kunden schlechte User Experience als Kaufargument anzudrehen. Oder ist es vielleicht einfach so, dass ein Kühlschrank mit Bluetooth nicht wegen des Bluetooth gekauft wird, sondern weil es keinen Kühlschrank in der Preisklasse ohne Bluetooth gibt? Sind wir

durch Zufall in eine merkwürdige Spirale der Gleichgültigkeit hineingerutscht, in der es uns Kunden egal ist, was für ein Technikschnickschnack in unseren Geräten enthalten ist, weil wir einfach nur das Gerät haben wollen, und in der es den Herstellern egal ist, was für Technikschnickschnack sie in ihren Geräten verbauen, weil die Geräte trotzdem gekauft werden?

Und noch viel wichtiger: Was tun die Hersteller, wenn sich irgendwann ein tatsächlich innovatives Gerät durchsetzt, das den Markt mit einer unaufhaltbaren Kraft überrollt, wie es einst das erste iPhone tat? Was tun wir, wenn wir eines Tages aufwachen und unsere bis dato zentrale Anlaufstelle für jedes Haushaltsgerät, unser Smartphone, plötzlich obsolet wird? Ist es tatsächlich „smart“, sein Leben um sein Smartphone herum aufzubauen und zu planen?

Selbst wenn die große Technologierevolution noch Jahrzehnte ausbleibt, und wir in diesem Zustand aus Ideenmangel und Nutzlosigkeit festhängen, so bleiben dennoch die offensichtlichen Probleme. Nahezu jeden Tag wird ein neues IoT-Gerät gehackt, weil selbst einfache Verschlüsselungsprotokolle nicht eingehalten werden. Als Kunde verkaufe ich meine persönlichen Daten an diverse mir nahezu unbekannte Firmen und weiß in der Regel nicht, welche kritischen Folgen das für mich haben kann, zumal ich für jeden neuen Hersteller mit einer eigenen App wahrscheinlich auch noch ein neues Kundenkonto anlegen muss. Zudem ist die zusätzliche Technologie nicht nur eine große Schwachstelle in der Sicherheit, sondern auch im eigentlichen Design. Das IoT ist kein elegant verarbeitetes Gimmick, es ist das Aushängeschild. Produkte werden in den Technologiemarkt gezwungen, selbst wenn die Technologie keinen echten Zweck hat. Es geht im Internet der Dinge nicht darum, den menschlichen Alltag mit seinen First-WorldProblems sinnvoll zu ergänzen, sondern darum, ein Produkt auf den Markt zu stellen, das seinen überhöhten Preis mit schlecht integrierter, merkwürdig zu bedienender, unsicherer Soft- und Hardware rechtfertigt.

Das IoT verändert unsere Welt nicht in innovativer, revolutionärer Art und Weise. Es gibt uns andere Lösungen für bereits gelöste Probleme, die häufig nicht besser sind, als die bereits bestehenden. Aber da die neue Lösung ein Smart-Device in sich trägt, scheint sie innovativ und unabdingbar. Das IoT ist somit kein Weltverbesserer, es ist eine Resignation. Wir finden uns mit unserem Alltag ab, indem wir immer neue Lösungen für dieselben Probleme schaffen, anstatt neue Probleme aufzustellen und diese zu lösen. In der Welt des IoT befinden wir uns in keiner technologischen Revolution, sondern in einer technologischen Gehorsamkeit. Wir arbeiten nicht auf eine Welt zu, in der Computer elegant und nützlich in unsere Umwelt auf natürliche Art und Weise verwoben sind, sondern auf eine Welt, die



Henning Neu, Datenschutz- und IT-Sicherheitsberater, praemandatum GmbH

sich mit unhandlicher und überflüssiger Soft- und Hardware brüstet. Aus der einstigen Vision des Ubiquitous Computing wurde ein unreflektierter Abklatsch. Somit spiegelt selbst der Name „Internet of Things“ die Essenz dieser Bewegung wider: Eine klobige Neuauflage einer bereits bekannten Idee.

Die Zukunft vorherzusehen, ist wie immer unmöglich, doch wenn ich daran denke, wie wir uns vor 30 Jahren die heutige Zeit vorgestellt haben, so bin ich manchmal enttäuscht. Echte Innovationen gibt es zwar hin und wieder in der Welt der Technologie, doch im Internet der Dinge finde ich sie nicht.

Henning Neu

Warum das „Internet der Dinge“ in den Marketingplan gehört

Es ist ein Graus für Marketingmanager. Waren es früher klar umrissene Aktionsfelder, spült heute die digitale Wirtschaft immer neue Themen auf die Agenda, die es zu bewerten und ggf. in den eigenen Plan zu integrieren gilt. Das „Internet der Dinge“ oder neudeutsch „Internet of Things“ (kurz IoT) ist einer dieser neuen Felder. Bevor wir aber die IoT-Bedeutung für das Marketing unter die Lupe nehmen, schauen wir uns einmal an, wie sich der Markt entwickelt. Denn wie auch viele andere digitale Entwicklungen berührt IoT eine Vielzahl an Branchen und Prozessen, mitnichten ist es ein Thema rein für „Techies“ und Nerds.

Wenn der Kühlschrank plötzlich im Internet surft

Das Internet der Dinge hält unter dem Oberbegriff „Smart Home“ Einzug in unsere Haushalte, unterstützt uns in unserem Büroalltag, hilft Produktions- und Logistikprozesse zu optimieren (Industrie 4.0), kann die Mechanismen im Gesundheitswesen (Smart Health) verändern und hat Einfluss auf die Welt der Mobilitätsangebote (Smart Mobility). Kurz: es gibt keinen Bereich, in dem IoT keine Rolle spielt. Und dabei überschlagen sich die Entwicklungen. Ein Beispiel: konnte man vor zwei Jahren auf der größten Elektronikmesse CES (Consumer Electronics Show) in Las Vegas die ersten internetfähigen Kühlschränke sehen, gehörten sie auf der letzten IFA in Berlin schon zum festen Angebotsbestandteil bei fast jedem Hausgerätehersteller. Und in fünf Jahren werden wir Schwierigkeiten haben, überhaupt ein Gerät ohne Netzzugang und Display zu bekommen.

Dabei werden diese Entwicklungen aus zwei Richtungen getrieben. Die erste lautet „Was geht, wird auch gemacht“: Das Internet der Dinge ist eine gigantische Experimentierwiese, alles was irgendwie machbar scheint, wird früher oder später ausprobiert. Das erscheint punktuell sinnbefreit, liefert aber in jedem Fall neue Erkenntnisse und Erfahrungswerte.

Und erscheint die Idee auch zunächst abwegig, kann sie vielleicht in einem anderen Nutzungskontext plötzlich ein spannender Lösungsansatz sein. Man sollte also so manch eine Initiative nicht zu früh belächeln. Auch wenn es beispielsweise um vernetzte Haarbürsten oder Angeldrohnen geht.

Die zweite Richtung ist, dass das eigentliche Ziel der IoT-Entwicklungen darin besteht, Abläufe, Interaktionen, Prozesse für den Nutzer zu vereinfachen. Hierzu gilt es Prozessabläufe zu analysieren und Vorteile durch vernetzte Geräte oder Produkte zu identifizieren und für sich nutzbar zu machen. Wenn also Geräte automatisch Verschleißteile analysieren und im richtigen Moment nachordern, werden Ausfalllücken und damit potentieller Nutzerfrust eliminiert. Eine gute Basis für eine lange Kundenbeziehung. Und damit auch eine tolle Chance, die man als Marke nutzen und nicht seinen Mitbewerbern überlassen sollte.

Fest steht: Beide Perspektiven treiben die Entwicklungen unaufhörlich voran. Warum und wie können nun Markenverantwortliche agieren, die Marktentwicklung aktiv mitgestalten und sich somit auch zukunftsfähig aufstellen? Dafür betrachten wir hier vor allem die Bereiche Smart Home und Mobility, also Umgebungen, die als Touchpoints für unsere Zielgruppen in der Regel hochrelevant sind.

„Dinge“ werden zu Touchpoints

Speziell für unser Zuhause kommen fast täglich neue smarte Produkte auf den Markt, aus bisher analogen Dingen des Alltags werden nun vernetzte, schlaue Systemmodule. Der bereits skizzierte Kühlschrank steht nicht nur künftig mit einem Touchscreen für unmittelbare Lebensmittelbestellungen zur Verfügung, er analysiert künftig auch Inhalte um selbstständig Einkaufslisten zu erstellen oder die gesundheitsbewusste Ernährung zu unterstützen.

Herdplatten und Backöfen lassen sich fernsteuern oder mit Sprach-Assistenten bequemer bedienen. Lichtkompositionen, Einbrecherschutz, Optimierung des Energieverbrauchs – heute bereits möglich, in Zukunft durch das massiv zunehmende Produktangebot omnipräsent. Und auch die Automobilhersteller haben längst eine Veränderung ihres Produktportfolios eingeleitet. Neben der Fahrzeugproduktion bringen sie sich als Serviceprovider in Position und betrachten Autos zunehmend als „Smartphones on wheels“. Neben originären Fahrzeugservices wie z. B. der temporären Freischaltung von Motorleistung oder Unterhaltungsangeboten, werden Hersteller auch externe Services entgeltlich in ihrer Fahrzeugumgebung einbinden. Versicherungen, Lieferservices – was das Herz begehrt und der Nutzer gut gebrauchen kann ist willkommen in der kommenden App-Ökonomie in Autos.

Was alle Touchpoints eint ist übrigens die zunehmende Steuerung der Umgebung über Sprachsteuerungssysteme wie Alexa, Siri oder Google Assistant.

Herausforderungen und Chancen

In beiden Umfeldern gilt es dabei grundsätzlich unterschiedliche Herausforderungen – die über eine einfache Bedienung hinausgehen – zu meistern. Verbraucher erwarten zusehends, dass „Maschinen“ mitdenken. Die digitale Steuerung – nett! Aber echte Vereinfachungen gelingen erst dann, wenn es gelingt, den jeweiligen Nutzer zu identifizieren, sein Profil zu kennen und zu schärfen und im Gegenzug vorausschauende Angebote zu unterbreiten. Dafür ist es notwendig, dass wir Nutzer-IDs generieren und möglichst lückenlos entlang der Customer Journey einsetzen, die Daten sind dann jederzeit in den Clouds gespeichert. Soweit die Theorie. Denn gerade die Hoheit über Schnittstellen zum Verbraucher – und genau das ist die User ID – als auch die Datenhoheit, gelten als kritische Erfolgsfaktoren der Zukunft. Kurz: da wollen alle dran und jeder versucht sich in Position zu bringen um Plattform-Giganten wie Facebook, Google, Apple und Amazon die Stirn zu bieten.

Neben der strukturellen Herausforderung – User IDs und Clouds-Services – gilt es die richtigen Angebote für die Zukunft zu entwickeln und zu implementieren. Anders als in der Vergangenheit, als in der Regel eindeutig definierte Spezialistenprofile für die Forschung und Entwicklung den Job erledigten, braucht man in diesem Entwicklungsumfeld weitaus mehr Fähigkeiten, die man versammeln muss und damit auch eine neue Art zu arbeiten. Neue digitale Services sind dabei nicht ausschließlich Aufgaben der Forschungs- und Entwicklungsabteilung, sondern auch der Trend zu „Advertising as a Service“ erweitert die Themenvielfalt auf der Marketing-Agenda. Da nicht mehr nur die Idee entscheidend für den Erfolg eines neuen Angebots ist, sondern vor allem die Art der Umsetzung und zum Teil auch die Geschwindigkeit, sind kollaborative Arbeitsweisen und mehr Agilität als in der Vergangenheit wichtige Erfolgskriterien. Produktspezialisten treffen dann auf Informationsarchitekten, Designer, Programmierer, Analysten, Querdenker. Und idealerweise sind auch Verbraucher schnell Teil des Teams, um sinnvolle Services für diesen neuen Markt zu entwickeln. Die Herausforderungen für das Marketing lassen sich de facto also nur mit interdisziplinären Task-Forces lösen, die mithilfe von Design Thinking Workshops, Rapid Prototyping und iterativen Entwicklungsprozessen schnell und in enger Zusammenarbeit IoT-Angebote – Hardware wie auch digitale Services – entwickeln können.

Manfred Klaus

Internet of Things (IoT) und unser Zuhause – durch Artificial Intelligence (AI) wird der Zero Click Sale möglich

Werden unsere beliebtesten Science-Fiction Filme bald Realität?

Vielleicht, denn IoT und AI sind ein starker Zukunftstrend und werden früher oder später auch in Ihrem Leben zu finden sein.

IoT & AI – Was ist das und wie funktioniert's?

Die Abkürzung IoT steht für die englische Bezeichnung „Internet of Things“. Damit ist die Vernetzung verschiedenster Geräte miteinander gemeint. Diese Gegenstände können sowohl virtuell als auch physisch sein und arbeiten unterstützend zusammen. Die Daten werden ohne menschlichen Eingriff ausgetauscht. Durch die eigenständige Kommunikation der vernetzten Teilnehmer-Geräte können Aufgaben für den Besitzer erledigt werden. Welche Aufgaben das sein können? Die Anwendungsbreite geht von reiner Informationsgewinnung (wie zum Beispiel „Wie wird das Wetter morgen?“) über Online-Bestellungen, aber auch Notfall-Funktionen (rufen der Rettung, etc.). Klingt kompliziert? Ist es nicht! Ein bekanntes Anwendungsbeispiel für IoT ist die bekannte Alexa, Google Home und Amazon Echo – aber dazu später.

IoT-Geräte, oder auch sogenannte „smart Objects“, werden bereits bei Verbrauchern, aber auch in der Industrie verwendet. In der Industrie geht es unter anderem um Maschinen und Sensornetzwerke, die miteinander kommunizieren. Im privaten Bereich tauschen Personen, Tiere, Haushaltsgeräte, Computer und viele andere „smart Objects“ Daten über das Internet aus.

Wie funktioniert nun so ein IoT-System? Zuerst benötigt jedes Gerät in einem IoT-System einen eingebetteten Prozessor, um ein „smart Object“ zu werden. Wichtig ist zusätzlich, dass jedes Gerät eindeutig in seinem Netzwerk identifiziert werden kann. Das kann durch die Zuweisung verschiedener Codes erfolgen. Daten, die dann ausgetauscht werden, können je nach Anwendung zum Beispiel Messwerte, Sensordaten von Bewegungsmeldern, Sprachdaten oder ähnliches sein. Die Daten werden lokal oder über eine Cloud (eine Speicherplattform) gespeichert und verarbeitet.

Nachdem IoT soweit geklärt ist, kommen wir zur nächsten vielleicht eher unbekanntem Abkürzung AI. AI bedeutet Artificial Intelligence, oder zu Deutsch künstliche Intelligenz (KI). Ziel des Forschungsgebietes der künstlichen Intelligenz ist es, das menschliche Denken auf Computer und Maschinen bestmöglich zu übertragen. Diese Geräte sollen also selbstständig Aufgaben lösen können. Beispiele hierfür sind Roboter. Norma-



Manfred Klaus,
Geschäftsführer/
Partner/Sprecher
der Geschäfts-
leitung, Plan.Net
Gruppe



Alexander Eser,
Co-Founder &
Managing Director,
kaufberater.io

lerweise ist ein Roboter nur so intelligent wie sein Programmierer. Es gibt allerdings bereits Roboter, die beispielsweise aus ihren eigenen Fehlern lernen, ohne zusätzliche Programmierung. Diese Roboter reagieren dann sozusagen intelligent und wiederholen einen einmalig begangenen Fehler nicht.

Das Forschungsgebiet der künstlichen Intelligenz wird grundsätzlich in vier Typen unterschieden. Rein reaktive künstliche Intelligenz reagiert lediglich auf ihre Umwelt oder Situation. Dieser Typ kann keine Erinnerungen bilden oder auf Erfahrungen zurückgreifen. Ein Beispiel ist IBMs Deep Blue, das den menschlichen Schach-Champion geschlagen hat. Der zweite Typ von KI sind Systeme mit begrenztem Gedächtnis. Diese stützen sich auf vergangene Informationen und Vorprogrammierungen. Beispiele sind selbstfahrende Fahrzeuge und Chatbots. Der dritte Typ sind Systeme, die Emotionen verstehen und darauf reagieren können. Der vierte Typ sind „ihrer selbst“ bewusste Systeme. Also Roboter mit einem eigenen Bewusstsein. Typ drei und vier kommen derzeit in Filmen vor, sind aber Ziel des Forschungsgebietes der KI.

Außerdem gibt es zwei Arten der KI, die starke und schwache KI. Bei der starken AI wird versucht eine Maschine zu entwickeln, die alles kann, was auch ein Mensch kann. Die schwache AI befasst sich damit, einzelne menschliche Fähigkeiten auf Maschinen zu übertragen. Beispielsweise das Erkennen von Sprache oder Texten.

IoT & AI – Was ist dabei Zero Click Sale?

Zero Click Sale bedeutet nichts anderes, als bestellen und bezahlen ohne einen einzigen Klick. Wie das funktioniert? Eben zum Beispiel mit der Sprachsteuerung über Alexa, Google Home und Amazon Echo. Durch die Vereinigung von KI und IoT könnten diese Geräte bald vielleicht sogar Produkte bestellen und zusenden, bevor wir überhaupt wissen, was wir brauchen. Die Interessen der Besitzer können durch diese smarten Objekte gespeichert werden und für nächste Bestellungen hergenommen werden. Dadurch kaufen Amazon Echo, Google Home und Alexa-Besitzer eindeutig mehr online, als andere Konsumenten. Allerdings kann eine Sprachsteuerung auch über unser Smartphone laufen, zum Beispiel über die Sprachassistentin Siri, S Voice oder Google Assistant. Domino's Pizza hat vor kurzer Zeit die Zero Click App vorgestellt. Dadurch wird mit einem einfachen „Hallo Siri, bitte öffne Zero Click“ und nach Ablauf eines 10-Sekunden-Countdowns die vorgeschriebene Lieblingspizza bestellt. Auch der Bezahlprozess kann bereits automatisch und im Hintergrund ablaufen. Die sogenannten Zero-Click-Payments in vielen Webshops haben die notwendigen Kun-

deninformationen vorgespeichert und somit kann vereinfacht bezahlt werden. Auch beim Amazon Dash-Button muss nur auf einen Plastikknopf gedrückt werden und vorgeschriebene Waren des alltäglichen Gebrauchs wie Waschmittel werden bestellt und automatisch bezahlt. Im physischen Store kann durch das Pilotprojekt Amazon Go mit dem Smartphone, KI, Kameras und Sensoren automatisch beim Verlassen des Geschäftes bezahlt werden.

IoT & AI – Wie wird's derzeit angewendet?

Durch die Kombination des Internets der Dinge und der künstlichen Intelligenz wird beides gleichzeitig reifer und auch günstiger. Beim IoT geht es primär um Daten und um das Verbinden von Geräten. Sollen diese Daten genutzt und Handlungen getätigt werden, müssen sie von intelligenten Geräten bearbeitet werden. Dafür sorgt die künstliche Intelligenz.

Einsatzgebiete sind zum Beispiel das sogenannte Smart Home. Die Beleuchtung und Heizung kann beispielsweise durch eine App am Smartphone oder auch automatisch geregelt werden. Bewegungsmelder und Sensoren für Vorhersagen von Feuer und Überschwemmungen sorgen für mehr Sicherheit und können notwendige Schritte automatisch tätigen. Auch Geräte wie Kühlschränke und Waschmaschinen können als smarte Objekte energieeffizienter arbeiten, Reparaturen vorherbestimmen und fehlende Produkte melden bzw. bestellen. Auch im Gesundheitswesen bringt vor allem E-Health (Übertragung medizinischer Werte) und Umgebungsin-telligenz (Anpassen von Temperaturen) Vorteile in der Vorsorge und Überwachung von Patienten. Für zuckererkrankte Menschen kann zum Beispiel der Blutzuckerspiegel überwacht werden und je nach dem Insulin automatisch abgegeben werden. Und auch in der privaten Fitness kommen diese Technologien unter anderem durch smarte Fitnessarmbänder zum Einsatz. In der Industrie werden durch IoT und AI Transportwege und -zeiten in Echtzeit überwacht, Maschinen können untereinander kommunizieren und Produktionen anpassen und durch Sensoren werden notwendige Reparaturen prognostiziert. In der Automotive-Technik kommunizieren Fahrzeuge und Infrastruktur miteinander und können Informationen über Verkehrssituationen und Informationen an die Kfz-Werkstatt senden und selbst Entscheidungen über nächste Handlungsschritte machen.

Durch die Verbindung dieser Technologien wird die Sicherheit und menschliche Gesundheit erhöht, während Energie, Zeit und Kosten gespart werden.

IoT & AI – Herausforderungen & Sicherheit

Bei der Sprachsteuerung mit Zero Click Sale kann unter anderem unabsichtliches, falsches

oder unautorisiertes Bestellen stattfinden. Ein viel größeres Bedenken ist allerdings die Weitergabe von enorm vielen persönlichen Daten und der damit einhergehende Datenschutz. Cyberkriminalität, Schwachstellen und Sicherheitslücken im System sind weitere Sorgenkinder. Richtlinien und Standards zu diesen Technologien sind noch in Entwicklung.

Wie kann ich mich schützen? Um privat abgesichert zu sein, empfiehlt es sich immer sichere Passwörter zu verwenden. Um Zugriffe auf ein System wie ein smart Home von außerhalb zu verhindern, können durch bestimmte Verschlüsselungen Zertifikate an die teilnehmenden Geräte vergeben werden, die eine vertrauenswürdige Kommunikation bestätigen. Das sogenannte Trusted Network Connect kann zum Beispiel Zugriffe analysieren und je nach dem Nutzer sperren. Um sicher zu gehen empfiehlt es sich in jedem Fall, sich um die verwendeten Geräte und ihre Sicherheit individuell zu informieren.

Die Zukunft von IoT & AI

Im Zuge dieser Technologien und weiteren wird bereits von der Industrie 4.0 gesprochen. Der Trend zur Individualisierung und zur flexiblen Produktion durch das Nutzen digitaler Technologien ist damit gemeint. Das Internet, Prozessoren, Sensoren, Datenaustausch und die Vernetzung verschiedenster Geräte ermöglicht selbststeuernde und intelligente Produktionen. Vorreiter, also Firmen, die wir in Zukunft aufgrund ihrer Innovationen im Auge behalten sollten, sind unter anderem BMW, Daimler und Tesla sowie Amazon, Google und diverse Start-ups.

Unsere Zukunft wird in jedem Fall durch diese und weitere Firmen und deren Innovationen vor allem im Bereich IoT und AI verändert. In unserem zukünftigen Leben sind wir nicht mehr weit davon entfernt, dass unsere Autos Benzin oder Diesel kaufen sowie bezahlen und unsere Kühlschränke die Milch. Selbstfahrende Autos könnten Staus verhindern und Parkplätze alleine suchen. Der Arzt kann über das Smartphone sofortige Handlungen mit dem Patienten durchführen und smarte Städte können möglicherweise über vernetzte Kameras Reparaturen durchführen und den Müll entsorgen. Auch die Wirtschaft wird verändert. Der stationäre Handel wird durch eCommerce und Zero Click Sale gewandelt. Neue Berufe entstehen und Arbeitsplätze werden ersetzt, die Produktion wird mehr und mehr automatisiert und individualisiert. Dadurch werden wieder Kosten reduziert, Konsumentenerfahrungen verbessert und neue Innovationen resultieren. Die Weltpolitik beschäftigt sich bereits mit IoT und AI, dem dafür notwendigen Infrastrukturausbau und der Sicherheit sowie der Transparenz.

Fazit – IoT & AI

IoT und AI verändern die Art wie Menschen, Geräte und Daten miteinander interagieren. Diese Technologien können und sollen vor allem eines: Den Menschen in allen Lebensbereichen unterstützen. Außerdem vereinfachen sie alltägliche Vorgänge wie zum Beispiel Einkäufe mit Zero Click Sale. Wir sind gespannt auf die Ergebnisse der weiteren Forschungen!

Alexander Eser

IoT – neue Handlungsfelder für die Landeshauptstadt München

München ist ein hervorragend aufgestellter Wirtschaftsstandort, dessen High-Tech-Sektor seit Jahren durch innovative Systeme im Bereich embedded Systems, künstliche Intelligenz und IoT international sehr gut positioniert ist. Für die Landeshauptstadt München fokussieren sich die dynamischen Entwicklungen im Bereich IoT derzeit insbesondere auf zwei neue Handlungsfelder:

- Smart City insbesondere in den Bereichen Mobilität und Energie
- Förderung des Ausbaus einer modernen, digitalen städtischen Infrastruktur (Breitbandausbau und Mobilfunk) als Voraussetzung zur erfolgreichen IoT Entwicklung in den ansässigen Unternehmen.

Während die Stadt bei ihren Aktivitäten im Bereich Smart City selber Anwender von IoT Technologien ist, versteht sie sich im Rahmen der Maßnahmen zum Infrastrukturausbau als Förderer der innovativen Münchner Wirtschaftsunternehmen, die wiederum IoT basierte, digitale Produktionsprozesse am Wirtschaftsstandort entwickeln und durchführen und dabei auf ultraschnelle, hocheffiziente und verlässliche Datenübertragungen angewiesen sind. Implementierungen findet sich z.B. in der Automobilindustrie, Telemedizin, Gebäudeautomatisierung, Wearables und Logistik.

Smart City

Smart City beschreibt einen urbanen Raum, in dem Menschen und die sie umgebende Technologie (Sensoren, Aktoren) unmittelbar miteinander agieren.

München startete Anfang 2016 das EU-Projekt „SMARTER TOGETHER“, welches unter anderem auf der Grundlage von IoT Technologien höchste Energieeffizienz und vernetzte Mobilität in der Stadt erreichen will. Gemeinsam mit elf Partnern aus Wirtschaft und Wissenschaft arbeitet die Landeshauptstadt München hierbei an Lösungen für die lebenswerte Stadt der Zukunft. Dabei sind das Bestandsviertel Neuaubing-Westkreuz (30.000 Einwohner) und das benachbarte Neubaugebiet Freiham (geplante 20.000 Einwohner) die Modellstadtteile in München.



Kurz Kapp,
Stellvertreter des
Referenten für Arbeit
und Wirtschaft und
Leiter der Wirtschaftsförderung,
Landeshauptstadt
München

Ziel ist es, nachhaltige Lösungen für eine zukunftsfähige Stadtentwicklung, Mobilität und Klimaschutz zu entwickeln. Neben der Erprobung neuer technischer Lösungen ist ein wichtiges Anliegen des Projekts, die Bürgerinnen und Bürger der Stadt mit einzubeziehen bei der Gestaltung ihrer Stadt der Zukunft.

Im Rahmen des Projektes wurden 2017 in Neuaubing-Westkreuz die ersten Straßenzüge mit intelligenten Lichtmasten ausgestattet. Mit installierten Sensoren können damit beispielsweise Informationen aus Umwelt, Wetter und Verkehr erfasst werden. Die so gesammelten Daten sind Grundlage verschiedener Anwendungen und mobiler Dienste, die das Leben im Quartier und darüber hinaus erleichtern sollen. Auch können Bewohner über die Smart City München App Informationen und Angebote im Stadtteil bequem abrufen. Zudem können diese Lichtmasten mit adaptiver, bedarfsgesteuerter Beleuchtung ausgestattet werden, um den Energieverbrauch zu reduzieren, sowie für mobile Endgeräte öffentliches WLAN (M-WLAN) in dem Bereich anbieten. Im Sommer 2018 werden außerdem die ersten vier der insgesamt acht geplanten multimodalen Mobilitätsstationen an den Start gehen. An diesen Stationen verknüpft die Münchner Verkehrsgesellschaft MVG das Kernangebot des Öffentlichen Personennahverkehrs (ÖPNV) mit zusätzlichen Mobilitätsbausteinen, wie beispielsweise E-Carsharing, Pedelects, lastenfähige E-Dreiräder und Ladesäulen für Elektro-Autos. Zusätzlich wird an zwei Mobilitätsstationen jeweils eine Quartiersbox integriert. Diese Boxen besitzen Raumtemperatur-, Kühl- und Tiefkühlmodule, die Unternehmen genauso wie private Nutzerinnen und Nutzer zur Verfügung stehen. Auch diese können mit der Smart City App angesteuert werden. Auch im Bereich Energie wird moderne IoT Technologie eingesetzt: Zum einen sollen „Smart-Home“-Elemente den Energieverbrauch der Haushalte bis zu 25 Prozent senken. Zum anderen wird ein innovativer Batteriespeicher Ende Februar 2018 seinen Betrieb aufnehmen. Über ihn wird überschüssige Energie in ein so genanntes Virtuelles Kraftwerk der Stadtwerke München (SWM) eingespeist. Das Virtuelle Kraftwerk ermöglicht die Vernetzung vieler Erzeugungsanlagen und trägt somit zur Stabilisierung überregionaler Netze durch intelligentes Lastenmanagement bei.

Darüber hinaus sind die beiden smart mobility-Projekte Civitas Eccentric der EU und

City2Share des Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) Beispiele für weitere IoT basierte Mobilitätsmaßnahmen in der Stadt.

Beim Projekt Civitas Eccentric wird ein neues integriertes Mobilitätskonzept für den Münchner Norden entwickelt. Dazu werden Maßnahmen in

den Bereichen Carsharing, Bike-Sharing, Elektromobilität, Multimodalität, Mobilitätsmanagement, City-Logistik, Verkehrssicherheit und deren Integration in die Stadt- und Verkehrsplanung erprobt und evaluiert. Hierbei wurde z.B. eine Mobilitäts-App für Seh- und Hörgeschädigte mit Indoor-Routing-Funktion entwickelt.

Das Ziel des Projekts City2Share ist die vielfältige Förderung von Elektromobilität. Dabei werden ebenfalls innovative Sensorik und Informationstechnologien entwickelt und eingesetzt und neue multimodale Informations- und Zugangssysteme vernetzt.

Aufbau einer IoT-fähigen, digitalen Infrastruktur

Eine zentrale Voraussetzung einer erfolgreichen Digitalisierung von Stadtgesellschaft und Wirtschaft ist die Existenz einer zukunftsfähigen Infrastruktur. München ist zwar diesbezüglich in einer guten Ausgangsposition, doch die Nachfrage nach Daten und Informationen steigt angesichts neuer technologischer Trends wie künstliche Intelligenz und dem IoT mit enormen Wachstumsraten an und die digitale Infrastruktur muss stetig ausgebaut und erweitert werden. Die Landeshauptstadt, Referat für Arbeit und Wirtschaft, übernimmt dabei die Koordinationsfunktionen zwischen der Stadt München und den Breitband – bzw. Mobilfunkanbietern. Aktuelle Anknüpfungspunkte sind:

- Die Stadtwerke München (SWM) sind eine hundertprozentige Tochter der Stadt. Die Stadt hat über dieses Tochterunternehmen den Ausbau des Glasfasernetzes energisch voran getrieben. Schon heute ist der Ausbau des Glasfasernetzes Münchens in Europa führend. Bis 2021 werden rund 70 Prozent der Münchner Haushalte und Gewerbebetriebe schnelle Internetanschlüsse zur Verfügung stehen und langfristig soll ganz München flächendeckend erschlossen werden.
- Die Deutsche Telekom entwickelt die Leistungsfähigkeit ihres bestehenden innerstädtischen Kupferkabelnetzes weiter, indem es die Vectoring-Technik im Nahbereich ausbaut. Die Landeshauptstadt München hat hier bereits die Gespräche zwischen der Deutschen Telekom und den verschiedenen betroffenen Referaten (z.B. KVR, Baureferat, Planungsreferat, Kulturreferat/Denkmalchutz) koordiniert.
- Der Ausbau des Mobilfunknetzes wird stetig vorangetrieben. Hier hat die Stadt schon erste Pilotprojekte für strahlenminimierende Kleinzellennetze durchgeführt und bewertet.
- Als eine zentrale Mobilfunkthematik für IoT wird aktuell der Standard 5G (Fifth Generation) entwickelt, der bis 2020 marktreif sein wird. Das Referat für Arbeit und Wirtschaft eruiert hier verschiedene Projekte im Rahmen des EU-Rahmenprogrammes Horizon 2020, die

sich explizit mit dem Bereich 5G beschäftigen. Ziel ist es, kurzfristig erste Pilot- und Anwendungsfelder zu testen, um anschließend einen zügigen Roll-out der entsprechenden digitalen Infrastruktur zu gewährleisten und die Realisierung dieses Standards am Innovationsstandort München zu unterstützen.

Mittelfristig sind in München Mobilfunkpilotprojekte, die 5G Übertragungsraten erforderlich machen, in zahlreichen Bereichen, z.B. bei Großveranstaltungen wie dem Oktoberfest oder Fußballspielen in der Allianzarena, für Testfelder des autonomen Fahrens und für Telemedizin, denkbar. Diese Projekte sind mit Partnern zu entwickeln und die notwendigen Schnittstellen zu Landeshauptstadt München sicherzustellen.

- München ist auf Bundesebene als Standort für den Digital Hub Mobility ausgewählt worden. Das hat zur Folge, dass sich hier Keyplayer des Münchner Mobilitätssektors zusammen gefunden haben, die gemeinsam Innovation und Technik wie z.B. Autonomes Fahren und Sharing-Konzepte vorantreiben. Auf der Basis dieser Vernetzungen und vor dem Hintergrund, dass das Zusammenführen und Vernetzen von verkehrsrelevanten Daten über verschiedene Verkehrsmodule enormes Potential zur Verbesserung der Mobilität in sich birgt, strebt die Landeshauptstadt München an, einen integrierten Datenpool aufzubauen. Anfang 2018 hat sich auf Initiative des 2. Bürgermeisters Herrn Josef Schmid ein Konsortium im Bereich Mobilität gebildet, das die Zusammenführung von Daten in einer gemeinsamen Datenplattform konzipiert und plant. An dem Projekt beteiligen sich sowohl die Verkehrsplanung der Stadt München, die SWM/MVG, als auch wichtige Unternehmen der Automotive- und der IT-Branche – allen voran BMW – und die Technische Universität München, im Laufe des Projektes werden weitere Teilnehmer hinzukommen. Zusammenfassend lässt sich feststellen, dass technologische Innovationen im Bereich IoT nicht nur die großen und mittelständischen Wirtschaftsunternehmen in den kommenden Jahren vor große Chancen ebensowohl wie Herausforderungen stellen, sondern auch Kommunen wie die Landeshauptstadt München. München wird in vielen seiner kommunalen Aufgaben wie z.B. Mobilität und Energieversorgung zunehmend als Anwender von IoT – Lösungen auftreten. Gleichzeitig ist die Stadt auch gefordert, den in München ansässigen Unternehmen wettbewerbsfähige Rahmenbedingungen bereit zu stellen. Sie sieht es deshalb als eine dringliche städtische Aufgabe, den Ausbau einer IoT-fähigen digitalen Infrastruktur weiter voranzubringen.

Kurz Kapp

IoT im Zusammenhang von Interoperabilität, Echtzeitanwendungen, Architekturen und sozialer Akzeptanz

Das IoT ist in aller Munde und das Interesse in der Industrie ist groß. Doch die wenigsten wissen überhaupt was es ist. Was bedeutet IoT und wie unterstützt es uns im täglichen Leben – aber vor allem in der Wirtschaft und Industrie? Ein Einblick zur Interoperabilität, Schwachstellen und sozialer Akzeptanz.

Durch Amazon Alexa, Philipps Hue und weiteren Smart Home Anwendungen bekommt das Internet of Things zum ersten Mal einen verständlichen Usecase. Jedes „Ding“ der Welt kann vernetzt werden und Daten in die digitale Welt senden sowie Befehle empfangen. So können Verbraucher ihre Lampen und Rollläden über Apps steuern. Das Auto wird über einen einzigen Knopfdruck vor dem Einsteigen vorgewärmt. Was im privaten Umfeld bei alltäglichen Dingen einfach nachvollziehbar ist, hält nur langsam Einzug in die deutsche Industrie.

Wie funktioniert das Internet der Dinge?

Das zu vernetzende „Ding“ muss zunächst mit einem Mikroprozessor ausgestattet sein, welcher über eine drahtlose oder kabelgebundene Schnittstelle Daten und Befehle sendet und empfängt. Das Senden und Empfangen der Daten erfolgt über beliebige Kommunikationstechnologien, wie z.B. WLAN, UMTS / LTE, RFID oder Bluetooth.

Ein einfaches Beispiel: Eine Gartenanlage wird mit Feuchtigkeitssensoren ausgestattet. Diese senden über Mikroprozessoren Feuchtigkeitsdaten an einen Server. Von hier werden die Daten an eine App gesendet, sodass der Benutzer stets über den Zustand der Anlage informiert ist. Die Sensoren und Mikroprozessoren sind bisweilen in immer kleineren und günstigeren Formen einfach zu beziehen und zu verbauen. [1]

Dies ist aber nur der erste Teil der Vernetzung. Über die App kann der Benutzer die Bewässerungsanlage steuern. Diese ist gleichermaßen vernetzt. Beide Datenpools werden auf dem Server miteinander verknüpft. Durch Regeln entsteht eine Handlungskette: Sinkt die Feuchtigkeit unter 40% wird automatisch ein Befehl an die Bewässerungsanlage gesendet, welche eine stärkere Bewässerung durchführt.

Diese hier beschriebenen Aktionen fallen unter das klassische IoT. Doch IoT kann mehr – durch äußere Daten, wie z.B. die des Wetterdienstes, können äußere Einflüsse mit einbezogen werden. So kann die Bewässerung automatisch gemäß der Wettervorhersage gesteuert werden – ganz ohne Eingriff des Benutzers. Zeigt ein Feuchtigkeitssensor einen zu geringen Wert an, liegt vermutlich ein Fehler in der Bewässerungsanlage vor. Der Benutzer erhält über



Markus Reichenberger,
Gründer und
Geschäftsführer,
minnt GmbH

das System einen Alert und kann rechtzeitig Fehlerbehebungsmaßnahmen vornehmen oder das System selbst kann diese triggern.

IoT – für wen oder was?

Übertragen auf die industrielle Fertigung findet der Begriff „Smart Factory“ in der sogenannten Industrie 4.0 Gebrauch. Hier geht es darum Maschinen und Anlagen zu verbinden um Daten zu lesen und Steuerungen in Echtzeit und ortsunabhängig durch zu führen.

Produktionsanlagen organisieren sich ohne menschliche Eingriffe indem sie untereinander kommunizieren. Produziert beispielsweise eine Maschine aufgrund von äußeren Einflüssen weniger Stückzahlen, kann automatisch eine andere Maschine an jedem beliebigen Ort der Welt mehr produzieren. Gleichzeitig wird der Zustand der Maschinen permanent überwacht (Condition Monitoring). Durch automatische Analysen können Engpässe oder Unterbrechungen in den Prozessen frühzeitig verhindert werden. So müssen Verschleiss- oder Ersatzteile nicht mehr vorgehalten werden, sondern können vorausschauend bestellt werden (Predictive Maintenance).

Im Bereich der „Smart Energy“ können durch intelligente Systeme Energieauslastungen bedarfsgerechter verteilt werden, sodass der Energiebedarf von Firmen und Städten signifikant reduziert werden kann.

Ein weiterer Anwendungsfall zeigt sich in der vernetzten Großküche. Mithilfe einer Vernetzung können sämtliche Geräte in einer Anwendung vom Küchenleiter ortsunabhängig verwaltet werden. Der Verschleiß von Bestandteilen, wie z.B. Abdichtungen, wird rechtzeitig angezeigt. Messwerte wie Temperatur und Luftfeuchtigkeit werden nicht nur visuell angezeigt, sondern die zugehörigen Geräte können auch von überall gesteuert werden.

So kann die IoT auf jede beliebige Branche übertragen werden. Überall, wo Maschinen im Einsatz sind oder Daten gelesen werden, zeigen viele Anwendungsfälle, dass IoT Effizienz steigern kann. Ganze manuelle Prozesse werden vereinfacht, indem teure Kommunikation, beispielsweise zwischen Menschen oder durch Eingaben in IT-Systeme wegfallen. Entscheidungen werden jederzeit maschinell getroffen und Überbrückungszeiten bei Fehlern fallen weg.

Akzeptanz-Probleme und Hürden der IoT

Wenn IoT doch eine solche Vielzahl von Anwendungsfällen findet, warum ist die Verbreitung noch so gering? Ein Blick auf die IoT-Verbreitung in Deutschland zeigt: Noch nicht einmal jedes zweite Unternehmen arbeitet mit IoT-Lösungen. [2]

Amerika gilt als Vorreiter der IoT-Technologien, fast 50% der IoT-Projekte finden auf amerikanischem Boden statt, nur 30% in Europa. [3]

Ein Problem des IoT sind veraltete Lösungen, die nur eine starre und wenig performante Kommunikation der Systeme über VPN-Verbindungen erlauben. Sind solche oft teuer eingeführten Systeme erst einmal in den Unternehmen angekommen, so sind sie nur schwer wieder zu ersetzen.

Die meisten Entscheider scheuen den Einsatz bisher auf dem Markt vorhandener IoT Lösungen aufgrund der geringen Flexibilität, d.h. aus Sorge vor Eingriffen in die Hardware-Systeme und teuren Umstrukturierungen. Laut einer EY-Studie beklagen fast sechs von zehn Entscheidern (59 Prozent) hohe Investitionskosten. Auch der Mangel an qualifizierten Mitarbeitern kommt hinzu. [4]

Das Kernproblem vieler IoT-Lösungen ist jedoch der wenig flexible Umgang mit unterschiedlichen Hersteller-Systemen. Maschinen und Controller sprechen unterschiedliche Sprachen, weil sie auf Basis unterschiedlicher Technologien aufgebaut sind. Dies führt zu einer Vielzahl von „Datentöpfen“ und einer ausbleibenden Interoperabilität der Systeme. Besonders wenn unterschiedliche Branchen aufeinander treffen, wie z.B. Energieversorgungs- und Automobilindustrie, ist die Sorge vor einer Vereinheitlichung des Informationsaustausches groß. So gelingt es zum Beispiel nicht, die Elektromobilität und die erneuerbare und dezentrale Energiegewinnung zusammenzuführen. [5]

Die Folge von unterschiedlichen Herstellersystemen sind Insellösungen. Jeder Hersteller bietet eigene Anwendungen um Daten zu lesen und Geräte zu steuern, eine horizontale Kommunikation der Systeme bleibt aus. Dies zeigt sich auch im Endkundenbereich, wo sich selten Heizung, Licht und Jalousien sinnvoll miteinander koppeln lassen.

Nicht zuletzt besteht besonders im deutschen Umfeld ein starkes Hemmnis durch Sicherheitsbedenken und dem Vorurteil, „smarte Maschinen“ seien angreifbarer durch die drahtlose Kommunikation.

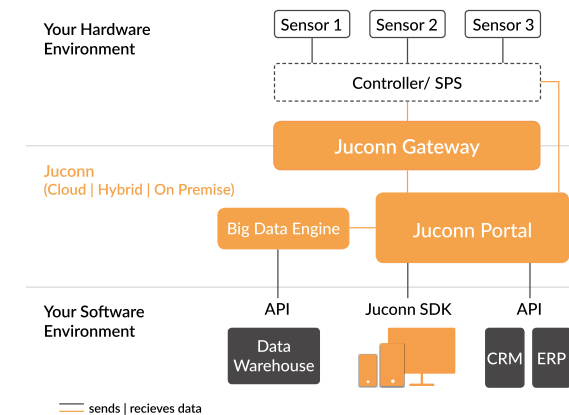
Was ist die Lösung?

Der weit verbreitete Gedanke, dass Maschinen unterschiedliche Sprachen sprechen, weil sie von verschiedenen Herstellern gebaut werden lässt sich durch moderne IoT-Technologien (z.B. juconn.de) aushebeln. Dadurch, dass die meisten gängigen Sensoren und Mikroprozessoren über Standard-Protokolle kommunizieren, unabhängig davon von welchem Hersteller sie stammen, können die Geräte problemlos miteinander kommunizieren. Die Kommunikation erfolgt dabei verschlüsselt und ist somit nicht weniger sicher als andere Systeme.

Mit Hilfe einer cleveren Systemarchitektur (siehe Grafik) und durch einfache plug-and-play-Anwendungen lassen sich die Geräte durch Einfügen eines Tokens in das Zielsystem in wenigen Schritten miteinander connecten.

Software-Architektur einer smarten

IoT-Anwendung



Die bereits bestehende Business Intelligence lässt den Anwender Regeln erstellen, um Daten auszuwerten, Alarime zu setzen und Befehle zu senden. So können Daten und Befehle einfach in Web- oder nativen Anwendungen verwaltet werden. Der Vorteil dieser modernen Technologien ist, dass in den meisten Fällen kein Eingriff in eine bestehende Systemlandschaft erfolgen muss und der Kosteneinsatz gering ist. Auf der anderen Seite sind die Systeme maximal flexibel was Schnittstellen-Integrationen, z.B. von Dritt-Systemen, externen Daten-Pools oder speziellen Gateways betrifft.

Im Beispiel der Gartenanlage lässt sich so die Bewässerungsanlage des Herstellers A einfach mit den Feuchtigkeitsfühlern des Herstellers B koppeln und erlaubt zusätzlich die einfache Integration der Wetterdienste.

Was heißt das für IoT in Deutschland?

Neue Technologien auf dem IoT-Markt machen hohe Investitionskosten verzichtbar, da sie einfache Lizenzmodelle anbieten. Das fachspezifische Know-How der Mitarbeiter ist nur begrenzt notwendig, da die Systeme smarte Bedienoberflächen bieten.

Besonders der deutsche Mittelstand sollte die Chance von modernen IoT-Lösungen nutzen. Entscheider dürfen sich dabei nicht scheuen, auf neue, moderne Technologien zurückzugreifen und somit kleineren, flexiblen Anbietern den Markt-Eintritt zu erlauben.

Besonders im Wettbewerb mit amerikanischen Unternehmen ist der Effizienz-Boost durch IoT-Lö-

sungen überlebenswichtig. Wenn Deutschland im internationalen Gefüge mithalten will, helfen clevere Systemarchitekturen signifikant Kosten einzusparen. Isolierte Insellösungen gehören so der Geschichte an – horizontale Lösungen sind der Schlüssel hin zu sinnvollen Anwendungsszenarien im industriellen Bereich sowie auf dem Endkundenmarkt, bis hin zur Smart City.

Markus Reichenberger

Referenzen: [1] Big Data Insider: Was ist das Internet of Things? <https://www.bigdata-insider.de/was-ist-das-internet-of-things-a-590806/> [2] CIO: Die größten Hürden für Internet-of-Things-Projekte <https://www.cio.de/a/die-groessten-huerden-fuer-internet-of-things-projekte,3572689> [3] IoT Analytics: The top 10 IoT application areas - based on real IoT projects <https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/> [4] CIO: Die größten Hürden für Internet-of-Things-Projekte <https://www.cio.de/a/die-groessten-huerden-fuer-internet-of-things-projekte,3572689> [5] Computerwoche: Industrie 4.0 ist das Internet der Ingenieure <https://www.computerwoche.de/a/industrie-4-0-ist-das-internet-der-ingenieure,2538117#>

1.4 IOT IN DER PRAXIS

1.4.1 Business IoT

Vom Produkt zum Service – organisatorischer Wandel als Voraussetzung für erfolgreiche IoT-Lösungen

Durch die Integration von „smarten“ Kommunikationstechnologien in Produkten ist es nun möglich, einen direkten Kontakt mit dem Kunden über die gesamte Nutzungsdauer zu etablieren und zu pflegen. Diese Konnektivität, die das „Internet der Dinge“ erst möglich macht, bietet große Chancen und stellt Unternehmen gleichzeitig vor immense Herausforderungen.

Die digitale Informationstechnologie sorgt zurzeit für eine tiefgreifende industrielle Veränderung. Nach dem schnellen Aufstieg des vierten Wirtschaftssektors (dem sogenannten „Informationssektor“) prescht die digitale Kommunikation auch in die übrigen Wirtschaftssektoren vor und stellt traditionelle Wertschöpfung zumindest in Teilen in Frage.

Dies spiegelt sich auch in der öffentlichen Diskussion wider. Vielverwendete Schlagworte wie „Industrie 4.0“, „Digitalisierung“ oder eben auch „Internet of Things“ („Internet der Dinge“) sind seit einigen Jahren die Dauerbrenner auf Fachtagungen und Messen in nahezu allen Wirtschaftszweigen. Dies ist nachvollziehbar und wenig verwunderlich. Die Auswirkungen der „Digitalisierung“ sind bereits heute überall sichtbar und für jeden unmittelbar erfahrbar. So werden energieautarke Gateways nicht nur im modernen Schienengüterverkehr eingesetzt, wo neben der Ortsbestimmung auch Temperaturen

und Schockaufkommen gemessen werden. Waggon und deren Ladung werden international überwacht und über die Auswertungen der Metadaten können Abläufe verbessert werden (http://www.boschengineering.de/en/de/einsatzgebiete/schiene/fahrzeuge/amra/amra_2.html). In der Landwirtschaft sorgt ähnliche Hardware für die Optimierung von Erträgen (<https://www.elektronikpraxis.vogel.de/sensorloesung-fuer-den-spargelanbau-ausgezeichnet-a-503938/>). Automobilhersteller werten zur Nachjustierung ihrer Produktion Flottendaten in Echtzeit aus (<http://www.boschconnectedvehicle.com/us/en/index.html>) und Gebäudereiniger wissen mittels Sensorik bereits, welche Räume am Tag besonders intensiv genutzt wurden, bevor sie das Gebäude betreten (<https://www.prnewswire.com/news-releases/data-driven-cleaning-services-closer-to-reality-with-intelligent-building-iot-solution-300392635.html>).

Diese neuen Einsatzformen von Informationstechnologien eröffnen spannende neue Möglichkeiten in einer immer stärker vernetzten Welt. Zugleich konfrontieren sie jedoch auch etablierte Unternehmen mit notwendigen organisatorischen Anpassungen. Dies zeigt sich auch zunehmend in unserer angestammten Domäne, der Automobil- und Zuliefererindustrie.

IoT verändert die Beziehung zum Kunden

IoT verändert über neue Geschäftsmodelle die Natur traditioneller Kundenbeziehungen. Das klassische produzierende Gewerbe ist hier ein gutes Beispiel: Die Zeiten, in denen das fertige Teil oder System vom Band gefallen ist und nach bestandener Qualitätsprüfung in „die freie Wildbahn“ entlassen wurde, sind in weiten Teilen vorbei.

Durch die Integration von „smarten“ Kommunikationstechnologien in Produkten ist es nun möglich, einen direkten Kundenkontakt über die gesamte Nutzungsdauer zu etablieren und zu pflegen. Die Konnektivität und die Software, die das „Internet der Dinge“ erst möglich machen, werden ein elementarer Bestandteil des Produktes und definieren in immer größeren Maßen die – auch vom Kunden erwartete – Leistungsfähigkeit und Funktionalität. Dies kann so weit gehen, dass die „smarten“ Funktionen und deren Nutzung komplett in den Vordergrund rücken und die eigentliche Hardware als Mittel zum Zweck angesehen wird.

Entsprechende Geschäftsmodelle, wie sie in der Unterhaltungsbranche bereits Standard sind (Musik- und Videostreaming), beginnen sich auch in der Automobilindustrie zu verbreiten. Mobilitätsangebote wie Car2Go oder DriveNow gehören hier wohl zu den bekanntesten Beispielen, wobei ähnliche Servicemodelle auch im Zuliefererumfeld Einzug halten. Diese neuen Geschäftsmodelle verlangen

natürlich auch ein Umdenken auf Kundenseite, wo in Zukunft Geldflüsse weniger für den Besitz als für die Nutzung fließen. Vornehmlich finden sich jedoch die größten Herausforderungen bei den etablierten Anbietern.

Die Grenzen zwischen Entwicklung und Produktion verschwimmen

Die Entwicklung und Herstellung von physischen Produkten ist naturgemäß ein zeitlich abgeschlossener Prozess. Nachdem eine Generation von Teilen entwickelt und auf den Markt gebracht wurde, schaffen es funktionale Erweiterungen und Anpassungen meist erst in folgenden Produktgenerationen in das Produkt. Entwicklungskosten und Komplexität verlangen oft nach hohen Absatzzahlen. Produktlebenszyklen verlaufen über mehrere Jahre.

Dies bestimmt in direkter Folge auch die Natur der Kunden- und Nutzerbeziehungen. Der Kunde kauft ein Produkt mit den darin enthaltenen Funktionen in einer einmaligen Transaktion. Abgesehen von eventuellen Wartungsterminen oder Marketingaktionen sind direkte Interaktionen mit dem Hersteller nicht vorgesehen. Die Erwartung ist, dass funktionale und qualitativ hochwertige Produkte für einen möglichst langen Zeitraum unverändert ihren vorher fest definierten Dienst tun.

Im Zeitalter des „Internets der Dinge“ ist der Nutzer im ständigen Austausch mit den Herstellern und ihren Produkten. Mit dem Internet verbundene Systeme und Sensoren senden Informationen über ihren Betrieb, ihre Nutzung und ihren Status an die „Cloud“ - also an Server, die die Daten speichern, weiterleiten, verarbeiten und über weitere Applikationen dem Kunden und dem Hersteller aufbereitet zur Verfügung stellen. In immer mehr Fällen funktionieren diese Kommunikationskanäle in beide Richtungen. So können Funktionen über Updates verändert oder sogar erst freigeschaltet werden (<https://www.theverge.com/2017/9/10/16283330/tesla-hurricane-irma-update-florida-extend-range-model-s-x-60-60d>).

Durch die bestehende Verbindung zu jedem im Feld befindlichen Produkt bekommt der Hersteller nicht nur einen genauen Status über die Nutzung und den Zustand seines gesamten verkauften Bestandes. Auch wird hierdurch eine Eins-zu-eins-Beziehung zu jedem Kunden über den gesamten Produktlebenszyklus möglich.

Die kontinuierliche Veränderung und Verbesserung der Produkte im Feld ist künftig durch „over-the-air“ Software Updates technisch möglich und wird damit zu einer Kundenerwartung werden – mit gravierenden Auswirkungen auf klassische Entwicklungs-, Absicherungs- und Produktionsabläufe.

IoT Produkte brauchen Serviceorganisationen

IoT Lösungen verlangen im einfachsten Fall eine ständige Pflege und Aktualisierung der gesamten Kette an wertschöpfenden Dienstleistungen. Steigende Datenmengen und neue Applikationen machen eine konstante Anpassung und Aktualisierung der eigenen Lösungen notwendig. Komplexere Systeme interagieren oft in einem Ökosystem mit einer Vielzahl anderer IoT Lösungen. Die Komplexität und Dynamik eines solchen Ökosystems hängt hier also nicht nur an der Funktionalität der eigenen Lösung, sondern auch an der Kompatibilität mit anderen Anwendungen von fremden Herstellern.

Von zentraler Bedeutung ist bei einem solchen globalen Netzwerk der Dinge stets auch die Daten- und Systemsicherheit. Wenn alles miteinander verbunden ist, ist auch alles ein potentielles Ziel von Spionage oder Sabotage. Anders als bei nicht-netzten Produkten, müssen daher System- und Sicherheitsupdates in schnellem Rhythmus durchgeführt werden.

Globale IoT Ökosysteme befinden sich so stets in einem Zustand der Veränderung und Anpassung. Beispielsweise kommen neue Softwarefunktionen hinzu, bestimmte Protokolle ändern sich oder eine neue Generation von Sensoren wird irgendwo auf der Welt gerade zum ersten Mal verkauft. Bestehende Lösungen sollten all diese Veränderungen berücksichtigen, wenn sie auch noch in Zukunft funktional bleiben und ihren Kunden Nutzen stiften sollen <https://www.networkworld.com/article/3093439/internet-of-things/throwing-our-iot-investment-in-the-trash-thanks-to-netgear.html>.

IoT Lösungsanbieter müssen also über den gesamten Produktlebenszyklus hinweg Kapazitäten vorhalten, die zum einen das System technisch up-to-date halten und zum anderen auf Kundenanfragen kompetent und zeitnah reagieren können. Kapazitäten meint in diesem Fall die Verschmelzung von Entwicklung und Betrieb in einer Abteilung, auch DevOps genannt, die die jeweiligen Systeme mit entwickelt hat und bei Problemen zeitnah unterstützen kann. Die generelle Aufrechterhaltung der Verfügbarkeit des Systems ist hierbei naturgemäß hochkritisch, da nachgelagerte wertschöpfende Aktivitäten davon abhängen.

Auch die internen Systeme und Prozesse sollten die neuartigen Geschäftsmodelle reflektieren. Wiederkehrende Zahlungen und Mietmodelle müssen korrekt verbucht und dokumentiert werden, unterschiedliche Betrachtungsweisen in Bilanz und GuV berücksichtigt sein. Auch die vertraglichen Rechte und Pflichten einer Servicebeziehung unterscheiden sich von denen einer traditionellen Käufer-Verkäufer-Beziehung.

Auf Seiten der Unternehmens- und Projektplanung werden neue Kalkulationsansätze notwendig. Die Profitabilität hängt nicht mehr nur an der Anzahl der verkauften Produkte, sondern auch an der Anzahl und Art der damit verbundenen Serviceverträge und deren Laufzeiten. Dem gegenüber stehen nun nicht mehr nur die direkten Produktkosten, sondern auch die zusätzlichen Aufwände, die über die Laufzeit aller Vorrausicht nach anfallen werden – beispielsweise für die Aufrechterhaltung des Betriebs.

Solche Modelle haben somit Auswirkungen auf die Unternehmenssteuerung und die Auswahl der ihr zugrundeliegenden Kennzahlen. Dies kann für ein bisher nach traditionellen Geschäftsmodellen wirtschaftendes Unternehmen speziell mit Hinblick auf Investitionsentscheidungen eine große Herausforderung darstellen. Umso wichtiger ist auch ein entsprechend angepasstes Controlling, welches projektspezifische Aufwände nach möglichst genauen Schlüsseln und Buchungsprozessen zuordnen können muss.

Nichts geht ohne Partner

Da die technische Diversität hinter IoT Lösungen sehr breit ist, macht es oft Sinn, sich einen oder mehrere Partner zu suchen, mit deren Hilfe man einen „Connected Service“ anbieten kann. Sei es die Bereitstellung von Server-Infrastruktur, die Implementierung von Datenbanken oder auch die Gestaltung einer intuitiven Nutzeroberfläche – oftmals liegen die Themen außerhalb des angestammten Kerngeschäfts.

Neben der Fähigkeit, den oder die richtigen Partner auszuwählen, ist hier insbesondere die Kommunikation mit dem jeweiligen Geschäftspartner von nicht zu unterschätzender Bedeutung. Diese beginnt bei der Beschreibung der eigentlichen Leistung und Gegenleistung, geht über die regelmäßige Abstimmung und Koordination bei Veränderungen innerhalb der IoT Wertschöpfungskette und endet bei dem Zuordnen von Zuständigkeiten im Falle von Eskalationen bei Kundenbeschwerden.

Für ein vertrauensvolles Partnermodell benötigt es klar definierte Schnittstellen und transparente Entscheidungswege. Hier können auch Unterschiede in der Unternehmensgröße und -kultur schnell zu Missverständnissen führen. Je komplexer die IoT-Gesamtlösung, desto wichtiger ist die Zuverlässigkeit der Partnernetzwerke. Versagt ein Element der IoT Wertschöpfungskette, kann das gesamte System ausfallen, zu schmerzlichen kommerziellen Verlusten führen und der Reputation aller Beteiligten erheblich schaden.

IoT zu Ende denken als Schlüssel zum Erfolg
Zusammengefasst bleibt hier der Aufruf, die



Dr. Thomas Lücking,
Business Development
Manager für
den Bereich IoT,
Bosch Engineering
GmbH

Euphorie und den Gestaltungswillen für neue IoT Lösungen auch auf notwendige interne Anpassungen der Organisation zu übertragen. In einer neuen vernetzten Welt der Dinge werden die oben angeschnittenen organisatorischen Fähigkeiten und Ressourcen DIE herausragende kritische Erfolgsgröße für jegliche unternehmerische Aktivität. Je früher wir die Komplexität von IoT Lösungen gesamtheitlich berücksichtigen und durchdenken, desto erfolgreicher werden wir die IoT Zukunft gestalten.

Dr. Thomas Lücking

Wie IoT-Geräte für Konsumenten nützlicher werden

Prognosen für den Bereich Consumer IoT gehen seit langem davon aus, dass in Zukunft viele neue smarte Endgeräte für den Verbraucher riesige Datenmengen produzieren werden. Von intelligenten Glühbirnen und intelligenten Schließsystemen bis hin zu Fitnesstrackern sind viele dieser smarten Geräte bereits Teil unseres Alltags geworden. Aber warum ist der große Boom bisher ausgeblieben?

Das Internet der Dinge heute: Schaffen wir genug Mehrwert für Verbraucher?

Schauen wir uns den heutigen Markt genauer an. Das Internet der Dinge (Internet of Things, kurz IoT) ist heute noch von Markensilos geprägt. Ein Anbieter, der in den IoT-Markt einsteigen will, entwickelt heute ein Gerät, kümmert sich um die Connectivity und muss zusätzlich auch die entsprechende App bauen, damit der Mehrwert für den Endkunden überhaupt entsteht. Auf dem Markt können wir beobachten, dass sich die Expertise der Unternehmen oft auf einen Bereich konzentriert und die Digitalisierung der Produktwelt insgesamt teilweise schwer voranzutreiben ist.

Eine große Chance liegt hier in der Entkopplung des Software- und Hardware-Marktes. Echter und vor allem skalierbarer Mehrwert für Endnutzer kann entstehen, dem die Gerätehersteller sich tatsächlich auf ihre Kernkompetenz, die Herstellung von Geräten, konzentrieren. Software-Entwickler können dann verschiedenste bestehende oder neue Apps mit Daten anreichern oder gar neue Services basierend auf IoT-Daten erschaffen.

Indem wir die Welt der vernetzten Geräte entkoppeln und Entwickler und Unternehmen in die Lage versetzen, Anwendungen zu schaffen, die die generierten Daten dann verwenden, können wir größeren Nutzen für den Verbraucher schaffen. Gerätehersteller könnten sich auf ihre Kernkompetenz konzentrieren, nämlich die Entwicklung hochwertiger Hardware.

Auf der anderen Seite, können Softwareunternehmen oder einzelne Entwickler durch die Abkopp-

lung von Produktkomponenten Anwendungen auf den Markt bringen, die Daten aus diesen unterschiedlichen Quellen nutzen. Dies würde zu einer Welle neuer Produkte und Business-Chancen führen. Auf dieser Seite ganz ohne die langen Herstellungsprozesse, um eine funktionale und qualitativ hochwertige Hardware auf den Markt zu bringen.

Nehmen wir einen beispielsweise einen Nutzer mit einem intelligenten Türschloss und einem vernetzten LED-Panel. Jedes Mal, wenn die mit IoT-Technologie ausgerüstete Tür benutzt wird, wechselt das LED-Panel seine Farbe von Bernstein (geschlossen und gesichert) zu Grün (von einem befugten Benutzer geöffnet) bzw. Rot (unbefugter Zugriffsversuch) und blinkt rot, wenn die Tür länger als eine voreingestellte Zeit offen steht. Es handelt sich um zwei Bauteile, die in dieser Kombination normalerweise nicht in einem Anwendungszusammenhang stehen. Mit kreativem Blick betrachtet ist jedoch ein nahezu unbegrenztes Spektrum an Möglichkeiten für einen Entwickler vorstellbar. Auf diese Weise kann jede zwei- oder mehrteilige Kombination von Geräten durch eine App verknüpft werden, die alle Datenströme nutzt, die von eben diesen Geräten kommen.

Verursachen wir nicht eher mehr Probleme für den Verbraucher?

Auch wenn der Konsument eine ganze Reihe von intelligenten Dingen besitzt, so ist doch jedes einzelne in seinem eigenen Markensilo eingeschlossen.

- Eine neue Marke auszuprobieren, bedeutet oft, eine weitere App herunterladen zu müssen, auch wenn es für den Nutzer die bessere Lösung wäre, die bisherige App für smarte Geräte zu verwenden. Und im Gegenzug brauchen wir nur an unseren Lieblings-Fitnesstracker zu denken: Momentan ist es einfach nicht möglich, mehrere Fitness- und Gesundheits-Apps mit einem einzigen Gerät zu nutzen.
- Manche Apps geben Daten schon frei und weitere Anwendungen, wie IFTTT, ermöglichen bereits die Vernetzung von unterschiedlichen Daten und Geräten - für den vollen Lösungsumfang ist allerdings IT-Wissen gefragt und die Vernetzung selbst kann für Endnutzer herausfordernd sein.
- Das Speichern von Daten aus der bisherigen Nutzung beim Gerätewechsel ist meist nicht ohne weiteres möglich, auch wenn inzwischen immer mehr Unternehmen die Möglichkeit des Daten-Downloads anbieten. Die im Mai 2018 in Kraft tretende EU-Datenschutzgrundverordnung (DSGVO) wird die Rechte und Möglichkeiten der Nutzer in dieser Hinsicht stärken und Anbieter begünstigen, die entsprechende

Prozesse automatisiert gestalten können.

- Der Verleih von Geräten wie zum Beispiel smarten Skiern und die Speicherung der von ihnen erzeugten Daten ist schwierig. Der ausleihende Nutzer muss entweder bei jedem einzelnen Anbieter ein Benutzerkonto einrichten oder darauf verzichten, seine Daten zu speichern.
- Das Teilen generierter Daten mit Freunden oder Fachleuten, z.B. dem Hausarzt, ist nicht möglich – es sei denn, die App unterstützt eine solche Funktion.

Zusammenfassend produzieren die vielen Einzellösungen und heutigen Mechanismen noch Barrieren in der Nutzererfahrung.

Übertragen der Datenhoheit auf die Verbraucher

Wie lassen sich die aufgezeigten Probleme damit lösen? Wir bei Telefónica NEXT nehmen das Thema Datenschutz sehr ernst und glauben, dass Nutzer selbst die Entscheidung darüber treffen sollten, was mit ihren Daten geschieht.

Das Benutzerkonto unserer IoT-Plattform Geeny wird es dem Nutzer erlauben, Daten verschiedener Geräte in einer gesicherten Umgebung zu speichern. Dabei ist wichtig, dass der Nutzer immer die volle Kontrolle über seine Daten behält. Das Konzept von Geeny ist damit bereits im Geist der Datenschutzgrundverordnung formuliert. Das bedeutet konkret, der Nutzer kann Freigaben für seine Daten flexibel erteilen oder entziehen, er kann er sie mit App-Anbietern seiner Wahl oder mit Daten anderer Geräte kombinieren und natürlich auch löschen. Wie Paypal für den Online-Einkauf, so stellt Geeny das Vermittlerkonto für IoT Daten bereit.

Neben dem technischen Aspekt spielen selbstverständlich auch rechtliche, infrastrukturelle und Sicherheitsüberlegungen eine Rolle. Nichtsdestotrotz wird die Idee dahinter sichtbar: dem Verbraucher die Wahlmöglichkeit über die Anwendungen und Geräte zu geben, die er nutzen möchte.

Dies erleichtert den am IoT-Projekt Beteiligten die Arbeit und ermöglicht es ihnen, sich auf ihr jeweiliges Fachgebiet zu konzentrieren. Ein klarer Vorteil ist, dass Hardwarehersteller intelligente Hardware bereitstellen können, ohne dass bei ihnen zusätzliche Kosten für die Entwicklung und Aktualisierung der Apps anfallen. Softwareanbieter können sich mit den Devices beschäftigen und einen darauf zugeschnittenen Mehrwert bieten, indem sie mobile Anwendungen für jeden Bedarf erstellen, die sowohl neu generierte als auch bereits vorhandene Daten verwenden.

So möchten wir mit Geeny ein Ökosystem bauen, dass es den Konsumenten unter Wahrung ihrer Datenhoheit ermöglicht, ihre Daten und Geräte bestmöglich für sich einzusetzen.

Hanna Pradler

Die smarte Brücke zwischen Produktion und Office

Informationen spielen eine zentrale Rolle bei der Umsetzung der Industrie 4.0. Dabei existieren sie längst losgelöst von strukturierten Quellen wie Dokumenten. Mithilfe eines Object Management System können über das Internet of Things beliebig viele oder komplexe reale Objekte wie Maschinen oder Produktionshallen virtuell definiert, verwaltet und somit als digitale Informationsquellen genutzt werden.

Ein Object Management System (OMS) ist ein vollständig autonomes, aber anbindungsfähiges System, das problemlos in die bestehende IT-Infrastruktur des Unternehmens integriert werden kann. Dazu werden zunächst physische Objekte mit einem Sensor ausgestattet – die Basis der smarten Vernetzung. Die Kommunikation und Interaktion von physischen und virtuellen Objekten erfolgt dann über die für kleine Datenmengen besonders geeignete und energieeffiziente Long-Range-Technologie, über Wi-Fi oder andere Internetprotokollverbindungen.

Die über die Sensoren gemessenen Daten sind faktische Angaben zu den Eigenschaften des physischen Objekts sowie zu seinen Funktionen bzw. seinem Verhalten. Die gesammelten Daten werden in ein Datacenter weitergeleitet. Hieraus liest das OMS schließlich die wesentlichen Informationen aus und definiert das physische Objekt als virtuelles Objekt. Über Open APIs lässt es sich in einem letzten Schritt mit einer Vielzahl dokument- und prozess-verarbeitender Systeme verbinden.

Verknüpfen mit Dokumenten und Prozessen

Man kann etwa als Basis-Option eine Produktionshalle als virtuelles Objekt definieren und mit konkreten Informationen verknüpfen wie Anschrift und Quadratmeterzahl. Dazu zählen aber auch Informationen über den eigentlichen Verwendungszweck, dass die Halle – wie Mietverträge, Rechnungen für Maschinen und schriftliche Sicherheitsmaßnahmen zeigen – für die Produktion von zum Beispiel Automobilteilen genutzt wird.

Einen Schritt weiter geht man, indem man das Objekt mit konkreten Prozessen innerhalb des Unternehmens verknüpft: Ein 3D-Drucker wird in der Produktionshalle mit einem Sensor ausgestattet, der an das OMS meldet „Patrone des Druckers mit der ID 123 ist leer“. Das System erkennt den Drucker als definiertes, virtuelles Objekt und ist wiederum mit einem Case Management System oder einer anderen prozessverarbeitenden Lösung des Unternehmens verbunden, sodass hier die flexible Vorgangsbearbeitung im Backoffice gestartet wird. Angebunden an die im Unternehmen genutzte ERP-Lösung kann der Drucker die Information „Meine Patrone ist leer“



Hanna Pradler,
Product Owner
Geeny, Telefónica
NEXT



Math Huntjens,
Information
Architect / Manager
Technology, BCT

eigenständig weitergeben und der zuständige Mitarbeiter erhält den Auftrag, eine neue zu bestellen und einzusetzen.

Langfristig kann an ein OMS auch eine M2M-Technologie angeschlossen werden, damit sich der 3D-Drucker eigenständig beim Zulieferer melden kann, um eine Bestellung aufzugeben. Der zentrale Punkt bleibt dabei die semantische Kontextanalyse, über die wirtschaftlich nutzbare Wissen generiert und die angebotenen Prozesse dem Verhalten des intelligenten Objekts angepasst werden können. Die künstliche Intelligenz des OMS sorgt dafür, dass aus den gesammelten Daten erkennbar ist, dass in den Wintermonaten mehr gedruckt wird als im Sommer, für den Zeitraum X also mehr Material benötigt wird.

Einfache Integration in bestehende IT-Strukturen

Als separate Softwarekomponente kann ein OMS über Open APIs an die bestehende IT-Infrastruktur angebunden werden und sorgt dafür, dass schneller auf die Anfragen der Objekte reagiert wird. Denn Objekte sollen so intelligent sein wie Mitarbeiter und eigenständig ihre Anfragen an das Unternehmen richten. Außerdem wird die Integration in bestehende Prozesse dadurch erleichtert, dass ein OMS wahlweise in Form einer Website, eines Portals oder einer App genutzt werden kann. Wichtig ist zudem, es flexibel den jeweiligen Bedürfnissen und Anforderungen anzupassen.

Sicherheitsaspekt

Durch die geschaffene Kommunikations- bzw. Interaktionsfähigkeit zwischen Nutzern und Systemen über neue Schnittstellen steigt der Austausch von Daten und Informationen erheblich. Für die Sicherheit sind neben dem Unternehmen auch Software-, Cloud- und weitere Anbieter verantwortlich, mit denen es zusammenarbeitet. Auf Entwicklerebene wird auf die Einhaltung spezifischer Maßnahmen nach den Methoden „Security by Design“ und „Privacy by Design“ geachtet. Mittels Identity Access Management wird zudem festgelegt, dass jedes definierte Objekt nur von autorisierten Mitarbeitern eingesehen werden kann.

Fazit

Für Industrieunternehmen bietet das Internet of Things spannende Chancen für einen Datentransfer, ein Monitoring und folglich die Kommunikation von Objekten mit Menschen – und untereinander. Mit einem Object Management System etablieren sie eine Lösung, mit der physische Objekte zu digitalen Informationsquellen werden. Das Ziel: Den Arbeitsalltag der Mitarbeiter zu

erleichtern, Prozesse effizienter zu steuern und miteinander zu verknüpfen sowie Informationen gewinnbringend zu nutzen.

Math Huntjens

Am Ende gewinnt immer der Kunde ...

Als Johannes Gutenberg 1460 den Buchdruck erfand ahnte er vermutlich nicht, was dies auslösen würde. Bereits 100 Jahre später gab es in Europa zahlreiche Zeitungen, ja sogar Romane, die sich mit dem Leben einfacher Leute auseinandersetzten. Das Wissen um die Welt, dass bis dahin ausschließlich den Schriftgelehrten und Klöstern vorbehalten war, wurde durch Zeitungen und Bücher zum Wissen für jedermann.

In der Digitalisierung stehen wir vor einer ähnlichen Revolution wie beim Buchdruck: Intelligenz ist nicht mehr nur dem Menschen vorbehalten, sondern „Dinge“ werden durch Daten und Algorithmen so intelligent, daß sie den Menschen in vielen Bereichen ersetzen können. An vielen Rezeptionen und Arztpraxen werden wir in Zukunft mit „Alexa & Co.“ kommunizieren, wenn wir Termine haben wollen, Rezepte brauchen oder einen Behördenantrag stellen müssen.

Es ist extremst schwer heutzutage die Geburtsstunde der „Digitalisierung“ festzuhalten, aber in meinen Augen war es der „Browser-Krieg“ zwischen Microsoft und Netscape ab 1995. Am Ende hat zwar der ungeliebte „Monopolist“ mit seinem Browser gesiegt, aber Netscape hinterließ seinen Quellcode des Communicators an die Internetgemeinde und initiierte damals indirekt die „Open source“-Bewegung. In der heutigen Zeit ist open source nicht mehr wegzudenken und dominiert zahlreiche Entwicklungen der Digitalisierung, leistungstarke Betriebssysteme auf Servern und PC's sind open source, R und Python sind open source – Programme mit einer weltweit besseren community an Helfern und freiwilligen Service-Mitarbeitern als die meisten teuren Analytic-Tools. Und sie tragen zu dem bei, was wir heute erleben – Digitalisierung ist nicht mehr eine neue Version von MS DOS oder Windows, sondern eine breite Bewegung von zahlreichen Unternehmen, deren Wettbewerbsvorteil nicht mehr nur schiere Größe, sondern Kundenvorteil ist. Deutschland hat auf diesen Trend erstmal „typisch“ deutsch reagiert. Als Antwort auf die Dominanz von Google und Co. Im Consumer-Bereich erfand man Industrie 4.0, statt dem Internet der Kunden, also erstmal das Internet der Dinge!

Gott sei Dank erweist sich auch diese Bewegung als ein Segen und ein Innovator, denn nunmehr können Dinge uns mitteilen, wie es Ihnen geht, was sie so tun, wer sie benutzt und wann sie müde sind und einen Service-Mitarbeiter brauchen. Zahlreiche Hersteller vermarkten IoT-Plattformen, die man

zum Datensammeln nutzen kann und zahlreiche Unternehmen und Startups stürzen sich auf die Auswertung der Daten und schaffen neue Services für Industriekunden. Dabei übersehen manche Industrie-Kapitäne und Hardware-Hersteller mit promillehaften Software-Umsätzen, wozu dieser Trend (weiter) führen wird: zu einer noch stärkeren Commoditisierung der Hardware und einer Beschleunigung der Innovation auf der Software-Seite. Auf der CES 2018 in Las Vegas stellte das Schweizer Startup Rinspeed mit dem Konzeptfahrzeug snap seine Vision der Mobilität der Zukunft vor. Das Fahrwerk als „Skateboard“ um von A nach B zu kommen und der Aufbau mit zahlreichen Möglichkeiten für innovative „user experience“. Ähnliche Wege geht auch Siemens Healthineers mit ausgewählten bildgebenden Geräten wie MR oder Computertomographie – durch den Austausch alter Komponenten und neuer Software können „Altgeräte“ deutlich modernisiert werden.

Wenn nunmehr immer mehr Maschinen- und Anlagen Ihre Zustände funken und Energie-Netze Ihre Auslastung über IoT steuern erfüllen Sie erstmal einen Zweck, den man früher mit industrieller Ersatzbeschaffung umschrieben hat: wenn eine Maschine (wirtschaftlich) abgeschrieben war, hat man sich die nächste Generation angeschafft.

Das IoT wird diese Investitionen deutlich zurückdrängen, denn Algorithmen, die Beschaffungsinvestitionen verlängern, werden eher gekauft werden, als neue Hardware und damit werden „Plattformen“ zum Gewinner im industriellen Geschäftsmodell. Damit sind nicht die heutigen IoT-clouds gemeint sondern die Analytics-Dienste und Geschäftsmodelle, die IoT-Daten nutzen und auswerten. Was aber braucht es um diese Daten auswerten intelligent zu können? Müssen diese Unternehmen viele Millionen in Fabriken und Anlagen investieren um sich dafür zu qualifizieren? Auf der untersten Ebene braucht es lediglich einen intelligenten Analysten mit einer Open-Source Software und einem „gemieteten“ Cloud-Zugang und diese Person wäre – vorausgesetzt er kennt die Geschäftsprozesse und die Sensorik der Geräte – in der Lage millionenschwere Ersatzinvestitionen zu beeinflussen. Hier müssten eigentlich die Alarmglocken in den Vorstandsetagen der deutschen Industrie und vor allem im Mittelstand läuten!

Den IoT-clouds droht daher das gleiche Schicksal der Telekommunikationsbetreiber: Ihre Dienste werden zur reinen „Datencommodity“ und extrem margenschwach sein, während sich das Geld mit AI-Algorithmen verdient wird.

Und der gute alte Dieselmotor? Wird vom commodity Elektromotor verdrängt. Und die gute alte Steckdose als nimmersatter Verbrauchskanal der Grosskraftwerke? Werden von mobilen Akkus und

intelligenten Ladevorgängen verdrängt.

Ich durfte 1995 zu den Hochzeiten des Browser-Krieges auf ein Seminar der Motorola-University. Einer der vortragenden Strategie-Professoren damals hatte sich viel mit dem Untergang von Geschäftsmodellen beschäftigt. Er hatte schon damals viele Beispiele parat, von Unternehmen, die es heute nicht mehr gibt, weil sie „Trends“ verschlafen haben. Gefragt, ob es denn in seiner Erfahrung eine „Erfolgsformel“ für das Überleben von Unternehmen gibt, antwortete er nur: „At the end, the endcustomer always wins...“

Christian Haas

Das Internet der Dinge im Versicherungsbereich

IoT ist da – wirklich?

Auf dem Weg zum Internet der Dinge (Internet of Things oder IoT) – bis 2025 werden 25 Milliarden Geräte weltweit vernetzt sein.[1] Auch für Versicherer klingen die Anwendungsfelder in der Theorie mehr als einleuchtend: mit vernetzten Häusern, Autos und sogenannten „Wearables“ kann der Versicherer bereits vor Eintritt eines Unfalls, eines Brandes oder einer chronischen Krankheit präventiv Einfluss nehmen, anstatt lediglich den entstandenen Schaden zu begleichen. Zudem können bestimmte Schadenfälle gänzlich vermieden sowie Kundenbedürfnisse besser erfasst werden, wodurch der Versicherer die Chance hat, öfter mit seinen Kunden in Kontakt zu treten. Zusammengefasst werden durch das Internet der Dinge kundennähere, erlebbarere, kostengünstigere und auch profitablere Versicherungen ermöglicht.

Warum hat sich das Internet der Dinge jedoch immer noch nicht etabliert und warum befinden sich auch die genannten Anwendungsfelder teilweise noch in den Kinderschuhen, obwohl vernetzte Häuser und auch Telematik im Fahrzeug zum Teil bereits seit Jahrzehnten möglich sind?

Phase 1 – Vernetzte Dinge und die klassische Versicherung

Versicherer, wie auch die Allianz, vermarkten seit einigen Jahren Versicherungsprodukte mit einem integrierten vernetzten Gerät. So werden beispielsweise Telematiktarife in der Auto- oder der Gebäudeversicherung angeboten, die aus einer klassischen Versicherungspolice, einem vernetzten Gerät und/oder einer App bestehen. Meist sind die Tarife auf bestimmte Zielgruppen, wie z.B. Fahranfänger oder bestimmte Risikogebiete, zugeschnitten und bieten Rabatte, wenn der Kunde das vernetzte Gerät installiert.

Das Geschäftsmodell funktioniert gut, wenn die Vernetzung einen hohen Hebel auf die Schadenkos-



Christian Haas, CEO, Data Engineers



Steffen Krotzsch, Head of Sales Allianz Segment bei Allianz Partners S.A.S

ten hat, z.B. durch vermiedene Unfälle oder Diebstähle in bestimmten Zielgruppen. Für die Breite des Geschäfts sind jedoch die zusätzlichen Kosten für das Gerät sowie der vom Kunden erwartete Rabatt in Summe vielfach zu hoch, um durch im Mittel geringere Schadenkosten gedeckt zu werden. Im Gegenzug sieht die Mehrzahl der Kunden bisher auch keinen Anreiz, einen höheren Preis für diese Produkte zu zahlen, oder die vernetzten Geräte aus eigener Tasche zu finanzieren. Dazu kommt, dass viele Kunden Bedenken bezüglich der Datensicherheit und der Privatsphäre haben und sich auch schon deshalb nicht für derartige Produkte entscheiden.

Phase 2 – Neue Geschäftsmodelle

Wird damit das Internet der Dinge für immer reduziert sein auf Anwendungsfälle für ausgewählte Zielgruppen?

Keineswegs, denn neue Geschäftsmodelle werden das Internet der Dinge und die Anwendungsfälle in hohen Kundennutzen übersetzen und damit viele der Barrieren ausradieren. Hierbei spielen drei Entwicklungsfelder eine entscheidende Rolle: 1. Aggregation von vernetzten Geräten, 2. Integrierte und On-Demand Produkte sowie 3. Ökosysteme und Plattformen.

Aggregation von vernetzten Geräten: wenn alle Geräte zu Hause vernetzt sind, möchte kein Kunde eine Vielzahl verschiedener Apps bedienen, um die Geräte zu steuern. Kunden wünschen sich eine einheitliche Bedienoberfläche oder Sprachsteuerung über alle Geräte hinweg. Amazon Echo Plus bietet bereits eine derartige Integrationsschicht und auch die Allianz arbeitet an einer Smart Home Lösung, die die Geräte vieler Hersteller auf einfache Weise aggregiert.

Integrierte und On-Demand Produkte: in Phase 1 war der Ausgangspunkt stets eine Versicherung, die um vernetzte Geräte erweitert wird. Der umgekehrte Fall ist mindestens ebenso interessant: im vernetzten Gerät ist eine Versicherung eingebaut, quasi „Intel inside“ für die Versicherung. Erste Produkte aus dieser Kategorie sind bereits in einigen Märkten verfügbar, wie z.B. Neos in England oder Cozify/LocalTapiola in Finnland. Auch On-Demand Tarife sind in diesem Zusammenhang zu nennen. Dies sind Versicherungen, die nur aktiv werden, wenn der versicherte Gegenstand genutzt wird, z.B. „pay as you drive (PAYD)“ – ermöglicht durch eine Vernetzung der Dinge.

Ökosysteme und Plattformen: Plattform-Geschäftsmodelle wie sie AirBnB, Uber oder WeChat nutzen und Ökosysteme rund um gewisse Themenbereiche wie beispielsweise Mobilität halten zunehmend auch in der Welt der Versicherungsunternehmen Einzug. So hat die Allianz vor kurzem angekündigt, Teile der Kernsysteme als Open Sour-

ce anzubieten, um ein Versicherungs-Ökosystem zu ermöglichen. Kernpunkt ist dabei, den Kunden noch umfassender betreuen zu können und die Versicherungsprodukte für Kunden noch lebensnah zu machen, z.B. durch einen Service-Marktplatz rund um die Themen Wohnen, Gesundheit oder Mobilität. Und natürlich spielen vernetzte Geräte jeweils eine tragende Rolle.

Das Internet der Dinge ist also noch nicht ganz da, zumindest hat es aus verschiedenen Gründen die breite Masse der Menschen noch nicht erreicht. Aber es wird kommen, getragen von neuen Geschäftsmodellen mit hohem Kundennutzen – auch und gerade im Versicherungsbereich. Steffen Krottsch

Referenzen: [1] IHS Quarterly, Q1 2014, The Internet of Things Episodes

1.4.2 Industrial IoT

Industrial Internet of Things (IIoT): rechtlicher Handlungsbedarf für Unternehmen

Wenn in der Tagespresse über das Internet of Things (IoT) berichtet wird, geht es meist um die Vernetzung „intelligenter“ Haushaltsgeräte (den Kühlschrank, der rechtzeitig frische Milch bestellt) oder „connected cars“, die große Datenmengen sammeln und damit auch Unfälle verhüten können. Eine wesentlich bedeutendere (R) evolution bahnt sich aber gerade in der Industrie an, in der das Industrial Internet of Things (IIoT) die Digitalisierung der Produktion beschleunigt und wie gleich noch gezeigt wird, spielt das Recht dabei eine Schlüsselrolle.

Während heute Fertigungsanlagen noch überwiegend als „stand alone“ Maschinen betrieben werden, arbeiten in der Fabrik der Zukunft Maschinen, die nicht nur untereinander, sondern auch mit externen Zulieferern und Kunden vernetzt sind und miteinander kommunizieren. Das hat viele Vorteile für beide Seiten und ermöglicht neue Geschäftsmodelle wie die vorbeugende Wartung von Industrieanlagen (Predictive Maintenance) oder auch Products as a Service, die ihre Instandhaltung und weitere Dienstleistungen bereits beinhalten. Anstelle eines einmaligen Verkaufs tritt zunehmend die zeitweise Überlassung von Maschinen, deren Abrechnung ähnlich wie bei Software as a Service Lösungen nach dem Umfang ihres Gebrauchs und der damit erzeugten Güter abgerechnet wird. Möglich wird das durch Sensoren, die ihre Messdaten während der gesamten Nutzung der Maschine an den Hersteller liefern, der dann genaue Aussagen darüber treffen kann, wann welche Ersatzteile benötigt werden und mit welcher Lebensdauer der Maschine gerechnet werden kann. Der Anlagenbetreiber kann damit

kostspielige Standzeiten vermeiden, während der Hersteller seine Produkte verbessern und zugleich neue Einnahmequellen erschließen kann. Häufig werden dabei aber die rechtlichen Aspekte nicht rechtzeitig berücksichtigt, auf die jedes Unternehmen die richtigen Antworten finden muss.

Wem gehören die Maschinendaten im Industrial Internet of Things?

Bevor Maschinendaten ausgelesen werden, um rechtzeitig Verschleißteile ersetzen zu können, muss die Frage geklärt werden, wem die Daten gehören und ob dafür die vorherige Zustimmung des Kunden als Maschineneigentümer und/oder Betreiber benötigt wird. Derzeit gibt es aber (noch) kein Eigentum an Daten, obwohl Maschinendaten oft wertvolle Unternehmensassets darstellen.

Wer die Kontrolle über seine Produktionsdaten behalten will, muss deshalb seine Anlagen nicht nur technisch absichern, sondern auch mit rechtlichen Mitteln dafür sorgen, dass er allein bestimmen kann, was mit seinen Maschinendaten geschieht und wer sie nutzen darf. Das ist allein mit einer üblicherweise verwendeten Vertraulichkeitsvereinbarung (dem Non-Disclosure Agreement, kurz „NDA“) nicht möglich, sondern bedarf eines Datennutzungsvertrages oder eines sogenannten Data Licensing Agreement (DLA) zwischen den Beteiligten. Dem Recht an Daten und damit auch den Verträgen die es regeln, kommt also entscheidende Bedeutung dafür zu, wer welche Daten zu welchen Zwecken nutzen darf.

Schutz von Geschäftsgeheimnissen im IIoT durch Industrial Security Agreements

Allein mit dem Abschluss solcher Data Licensing Agreements ist es aber nicht getan. Unternehmen, die sich das Industrial Internet of Things zunutze machen wollen, müssen auch daran denken, sich vor ungewollten Datenabflüssen an Wettbewerber und Produktpiraten zu sichern. Nach einer Studie des Branchenverbandes Bitkom sind über die Hälfte aller deutschen Unternehmen in den vergangenen zwei Jahren Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Den dadurch entstandenen Schaden beziffert der Verband auf 110 Milliarden Euro. Mittlerweile betreiben auch viele Geheimdienste aktive Industriespionage und investieren hohe Summen, um ihrem Land im Wettlauf um neue Technologien einen der vorderen Plätze zu sichern.

An die Anlagensicherheit wird aber in deutschen Unternehmen noch viel zu wenig gedacht und wenn dies doch geschieht, fehlt es häufig dennoch an einem zumindest ausreichenden Sicherheitsniveau bei den Datenempfängern. Nur wenn in der gesam-

ten digitalen Supply Chain vergleichbare Maßnahmen für eine sichere Produktion getroffen werden, können teure Datenverluste vermieden werden. Das verlangt auch der Schutz von Geschäftsgeheimnissen, der nach der neuen EU-Know-how Schutzrichtlinie nur noch gewährt wird, wenn die betroffenen Informationen angemessenen Geheimhaltungsmaßnahmen unterworfen wurden. Das bedeutet, dass vertrauliche Geschäftsinformationen nur noch dann der gesetzliche Schutz für Geschäftsgeheimnisse zuteilwird, wenn sie mit technischen Mitteln und vertraglichen Vereinbarungen vor einer rechtswidrigen Nutzung geschützt wurden. Dazu müssen mit allen Partnern in der gesamten Lieferkette Industrial Security Agreements (ISA) geschlossen werden, die ein einheitliches Schutzniveau sicherstellen. Das ist nicht trivial und erfordert immer individuelle Lösungen, da nicht alle Daten und Geschäftsinformationen denselben Schutz benötigen und Zulieferer oder Dienstleister ihre eigenen Schutzkonzepte entwickelt haben, die sich nicht immer mit denen ihrer Auftraggeber decken und gravierende Lücken aufweisen können. Nur wenn Recht und Technik ineinandergreifen und der Anwalt nicht zu spät eingebunden wird, lassen sich Lösungen finden, die nicht nur die „Compliance“ gewährleistet, sondern dafür sorgen, dass aus Daten auch Produkte werden können. Wenn dann physische Produkte und Daten in neuen Product-Service Systems (PSS) vereint werden, erfordert das auch geeignete Verträge, mit denen die daraus entstehenden Rechte und Verantwortlichkeiten geregelt werden.

Nutzung personenbezogener Daten im Industrial Internet of Things

Schließlich werden im IIoT häufig auch personenbezogene Daten ausgetauscht. Das ist aber nur dann zulässig, wenn es eine gesetzliche Erlaubnis dafür gibt oder die betroffenen Personen darin eingewilligt haben. Auch Maschinendaten sind oft mit personenbezogenen Daten, etwa über den sie bedienenden Mitarbeiter verknüpft und können erst dann genutzt werden, wenn die datenschutzrechtlichen Konsequenzen bedacht wurden. Wer heute noch meint, dass Datenschutzverstöße lediglich ein Kavaliersdelikt darstellen, wird sich bald auf unangenehme Überraschungen einstellen müssen, denn ab 25. Mai 2018 ist die Europäische Datenschutzgrundverordnung (DSGVO) anzuwenden, die in solchen Fällen Geldbußen von bis zu 20 Millionen Euro oder 4% des (konzernweiten) Jahresumsatzes vorsieht. Um dem zu begegnen, muss der Schutz personenbezogener Daten schon bei der Produktentwicklung berücksichtigt werden („Data Protection by Design“) und auch in der Produktionsstraße umgesetzt werden.



Dr. Andreas Leupold,
Rechtsanwalt,
Leupold Legal

Neue rechtliche Herausforderungen in der Fabrik der Zukunft

Anlass den Datenschutz in die Geschäfts- und Produktionsprozesse zu integrieren bietet vor allem eine noch junge Entwicklung im Industrial Internet of Things: Dort gelangen nämlich zunehmend Assistenzsysteme zum Einsatz, die der Unterstützung der Mitarbeiter bei der Herstellung von Produkten dienen sollen. Je mehr sich diese Systeme durchsetzen, umso mehr personenbezogene Daten fallen dabei aber auch an. Wenn etwa der Arbeitshandschuh mit einem Barcodescanner ausgestattet ist, der die Arbeitsschritte seines Trägers aufzeichnet, dann muss vor dem ersten Einsatz geprüft werden, ob es dazu der Einwilligung des Arbeitnehmers oder eines Betriebsratsbeschlusses bedarf. In der Fabrik der Zukunft kommunizieren Bauteile mit dem Monteur und geben ihm eine akustische und/oder sensorische Rückmeldung, wenn sie fachgerecht verbaut wurden. Heute noch rein lokale Arbeitsplätze in der Fertigungsstraße werden mit anderen Standorten vernetzt sein, sodass ein Monteur in Asien und sein deutscher Kollege mittels Übertragung von Augmented Reality Daten und anderen Technologien zusammenarbeiten können, ohne ihre Produktionsstätten verlassen zu müssen. Die Vorteile einer derart vernetzten Produktion, die durch das Industrial Internet of Things erst möglich wird, liegen auf der Hand: weniger Fehler bei der Endmontage, was auch eine teure Produkthaftung vermeiden hilft, eine verbesserte Qualitätskontrolle und nicht zuletzt weniger Arbeitsunfälle sind nur einige davon. Das Beispiel verdeutlicht aber zugleich, dass Maschinendaten und personenbezogene Daten oft nicht mehr zu trennen sein werden und tiefe Einblicke in die Produktion zulassen, die nur den dazu befugten Personen gewährt werden sollten. Dazu bedarf es einer ganzheitlichen technischen und rechtlichen Absicherung, die alle Datenflüsse im Unternehmen und der Supply Chain erfasst.

Die digitale Welt ist und bleibt also voller Herausforderungen, die nicht mit altbewährten Methoden bewältigt werden können, sondern neue Lösungen erfordern, die unterschiedliche Disziplinen wie Recht, Wissenschaft und Technik zusammenführen müssen, damit Unternehmen wettbewerbsfähig bleiben und die deutsche Industrie ihre in vielen Bereichen errungene Marktführerschaft nicht verliert. Smart Production verlangt Smart Solutions, bei denen die Rechtsabteilungen und externe Berater frühzeitig eingebunden werden, um intelligente Lösungen zur rechtlichen Absicherung zu konzipieren und umzusetzen, damit Innovationen ihre gewünschte Wirkung erzielen können.

Dr. Andreas Leupold

IIoT-Plattformen sind Voraussetzung für Industrie 4.0

In der Fertigungsindustrie spielt das Industrial Internet of Things (IIoT) künftig eine Hauptrolle. In Deutschland nennen wir dieses Konzept Industrie 4.0. Hochkomplexe, automatisierte Produktionsmaschinen und Roboter werden untereinander und unternehmensübergreifend miteinander vernetzt. Dadurch entstehen standortübergreifende, flexible Produktionssysteme, die nicht nur automatisch fertigen, sondern auch sich selbst steuern und weitgehend selbst warten können. Allerdings dürfte es noch eine ganze Zeit dauern, bis die IIoT-Konzepte weitgehend realisiert sind. Doch die Unternehmen arbeiten mit einigem Aufwand daran. Die Unternehmensberatung PwC schätzt in einer aktuellen Studie, dass die deutsche Industrie in den nächsten fünf Jahren durchschnittlich 3,3 Prozent ihres Jahresumsatzes in Industrie 4.0-Lösungen investiert. Dies entspricht fast 50 Prozent der geplanten neuen Ausrüstungsinvestitionen und einer jährlichen Investitionssumme von mehr als 40 Milliarden Euro bezogen auf die gesamte deutsche Industrie. Damit Industrie-4.0-Anwendungen funktionieren, müssen Unternehmen unter anderem in sogenannte IIoT-Plattformen investieren, die die Maschinen mit dem Internet verbinden, sie absichern, analysieren, steuern sowie die notwendigen Schnittstellen für den Zugriff auf Applikationen und andere Systeme bereitstellen.

IIoT-Plattformen können aus Aufzügen Personenbeförderungssysteme mit garantierten Service Level Agreements machen. So das Beispiel MAX - eine präventive Service- und Wartungslösung von thyssenkrupp Elevators, die auf Microsofts IoT Azure Suite basiert. MAX arbeitet in Echtzeit, erstellt Prognosen und sorgt seinen Entwicklern zufolge dafür, dass Aufzüge 50 Prozent weniger oft aufgrund von Wartungsarbeiten stillstehen.

Mit dieser IIoT-Lösung reduziert thyssenkrupp Elevators nicht nur die Downtime seiner Aufzüge und verkürzt damit die Zeit, die Menschen damit verbringen müssen, auf Lifte zu warten. Gleichzeitig bekommt das Unternehmen einen Strom von Echtzeitdaten, die es auswerten kann, um seine Produkte laufend zu verbessern. Aufgrund der präventiven Wartung kann sehr viel besser geplant werden und Servicetechniker lassen sich deutlich effizienter einsetzen. Es können neue Geschäftsmodelle angeboten werden, zum Beispiel in Richtung Aufzug „as a Service“ mit Service Level Agreements, die nicht nur auf die „Meantime between failure“ ausgerichtet sind, sondern zum Beispiel auf die Zahl transportierter Gäste pro Stunde.

Das ist nur ein Beispiel dessen, was Unternehmen mit Hilfe von IIoT-Plattformen erreichen

können. Doch alle Szenarien drehen sich um höhere Produktivität, mehr Effizienz, mehr Flexibilität, mehr Innovation und natürlich um neue Geschäftsmodelle, die durch ihre Plattformen ermöglicht werden.

Die Elemente der IIoT-Plattformen

Grundlage für das Potenzial dieser IIoT-Plattformen, an denen mehrere hundert IT-Anbieter, Maschinenbauer, Automatisierungs-Spezialisten und große Systemintegratoren zumindest mitentwickeln, sind im Grunde IT-Standardfunktionen, die allerdings durch das Einbringen konnektierter Sensoren und Aktuatoren zu mächtigen Anwendungssystemen ausgestaltet werden können. IIoT-Plattformen verbinden die physische Welt mit der virtuellen Welt der IT und lassen so ganz neue Daten-basierte Geschäftsmodelle und Wertschöpfungssysteme entstehen.

Das Analystenhaus Forrester Research beschreibt folgende fünf Standardfunktionen von IIoT-Plattformen:

- **Connect:** Ein IIoT-Device, zum Beispiel eine Werkzeugmaschine, der Stromzähler in einem Haushalt oder eine Offshore-Windturbine in der Deutschen Bucht muss mit dem Internet verbunden und der Link gemanaged werden. Dazu werden typischerweise Funktechniken wie ZigBee, Z-Wave und andere stromsparende Wireless Personal Area Network-Technologien genutzt. Aber auch Mobilfunkanbieter bieten Machine to Machine (M2M) Kommunikationslösungen an, die Daten über ihre Mobilfunknetzwerke in entsprechende Rechenzentren oder in die Cloud transportieren.
- **Secure:** Die eingebundenen Security Devices und die von ihnen übertragenen zum Teil sensiblen Daten müssen vor Attacken geschützt werden. IIoT-Plattformen müssen daher Sicherheitskomponenten aufweisen, die Devices authentifizieren, Netzwerkverbindungen schützen, Software aktualisieren sowie Identity- und Access-Management übernehmen und Schutz vor Datenverlust bieten.
- **Manage:** Häufig bestehen IIoT-Lösungen aus Tausenden verbundener Geräte, um Betriebszustände wie Temperatur, Drücke, Vibration und anderes zu messen und zu steuern. IIoT-Plattformen bieten daher Funktionen, um die Device-Parks remote zu überwachen, zu testen, Software zu aktualisieren und Fehler zu beheben.
- **Analyse:** Die IIoT-Analyse-Funktionen entwickeln sich derzeit erst. Es geht um Daten-Filtrierung oder Streaming Analytics, damit sich Daten in Echtzeit monitoren lassen. Darüber hinaus können fortgeschrittene Analysen ge-

fahren werden, mit denen sich versteckte Muster und andere Einsichten in den verfügbaren Informationen finden und Aktionen anstoßen lassen können.

- **Build:** Die Unterschiedlichkeit der IIoT-Anwendungsszenarien verlangt Software-Integration und APIs (Programmierschnittstellen), um die herkömmlichen Business-Prozesse und Applikationen zu unterstützen. So muss schließlich ein Smart-Home- oder Smart-Energy-Service über ein klassisches ERP-System (Enterprise-Resource-Planning) abgerechnet werden können. IIoT-Plattformen vereinfachen die Entwicklung von Programmen und Geschäftslogiken. Sie geben Entwicklern Funktionen für Datenmanagement, Connectivity und Security. Außerdem bieten viele Plattformen Entwicklungs- und Scripting-Tools, API Links und API Management Tools, um IIoT-Anwendungen mit den Enterprise-Applikationen zu verbinden.

Der Markt wächst rasant

Dem Markt für IIoT-Plattformen attestieren Marktforscher glänzende Aussichten. Laut Forrester-Umfragen nutzen 60 Prozent der weltweit global tätigen Unternehmen bereits IIoT-Anwendungen oder planen sie einzusetzen. Bei allen anderen Firmen liegen die entsprechenden Nutzungswerte bei 52 Prozent.

Ebenfalls sprunghaft ansteigen wird den Marktforschern von IHS zufolge die Zahl der installierten IIoT-Devices. Betrug die installierte Basis 2015 rund 15,4 Milliarden mit dem Internet verbundene Geräte, so soll sie bis 2025 auf 75,44 Milliarden Devices steigen.

Den weltweiten Plattform-Markt schätzen die Analysten der renommierten Marktforscher von IoT-Analytics 2016 auf 417 Millionen Dollar. Bis 2021 prognostizieren sie ein Marktvolumen von 1,64 Milliarden Dollar, das bedeutet einen durchschnittlichen jährlichen Anstieg von 33 Prozent.

Allerdings wird sich die Zahl der Plattform-Anbieter in den nächsten Jahren laut IDC konsolidieren. Im Moment kommen zwar ständig neue IIoT-Plattformen auf den Markt, aber Mark Alexander Schulte, Senior-Consultant beim amerikanischen Marktforscher, erklärt: „Wir prognostizieren, dass langfristig nur 5 bis 6 Plattformen den IIoT-Markt dominieren werden. Für Anbieter also höchste Zeit, ihre bestehenden Dienste stärker an den Bedürfnissen ihrer Kunden auszurichten.“

In einer im Herbst 2017 von IDG durchgeführten Umfrage unter 385 IT-Entscheidern - hauptsächlich aus dem produzierenden Gewerbe - halten 57 Prozent der Befragten IIoT-Plattformen für eine unverzichtbare Technologie. Eingesetzt wird sie bereits



Falk Senger,
Geschäftsführer,
Messe München
GmbH

von rund 22 Prozent der Befragten. Im Zusammenhang mit IoT erklärten die Befragten Security-Technologien (53 Prozent) und Cloud Computing (48 Prozent) ebenfalls für unverzichtbar. In der gleichen Untersuchung schätzten 64 Prozent der Befragten die Bedeutung von IoT für das eigene Unternehmen als „sehr hoch“ oder „hoch“ ein.

Die Digitalisierung in der Produktion steht auch im Fokus der automatica 2018, die vom 19. Juni bis 22. Juni 2018 in München stattfindet. Der Themenbereich IT2Industry wird zeigen, wie komplexe hochautomatisierte Fertigungsmaschinen und Roboter „intelligent“ mit modernster IT und Internet-Konnektivität verbunden werden können. Das Ziel ist, die niedrigen Kosten der Massenfertigung mit der großen Kundennähe und Individualität der Lösungen von Handwerksbetrieben oder Manufakturen zu erreichen. „Plattformen und Ökosysteme“ spielen dabei eine wichtige Rolle und werden sowohl im Themenbereich IT2Industry als auch im Messe-Rahmenprogramm praxisnah aufgegriffen.

Falk Senger

Industrial Internet of Things: wie der Fertigungsablauf mittels Edge Computing intelligent gesteuert wird

Die digitale Simulation einer Produktionsstätte in Echtzeit bietet enorme Vorteile: Schon aus rein wirtschaftlicher Sicht bietet eine nahtlose Integration von Planung und Ausführungsdaten gute Aussichten auf schnellere Durchlaufzeiten, kürzere Maschinenanlaufzeiten und einen flexibleren Einsatz von Ressourcen und Fertigungsinseln.

Doch auch in puncto Planungs- und Produktqualität winken große Schübe. Nicht nur weil eine verbesserte Nachbearbeitung und weniger Verluste durch Fehler in der IT zu erwarten sind. Ein Datenaustausch zwischen realer und virtueller Fabrik führt im Idealfall dazu, dass sich beide Seiten synchronisieren und sogar gegenseitig kalibrieren.

Wie eine solche Fabrik und ein hierfür geeigneter Architekturansatz für Shopfloor und Edge Computing aussehen kann, haben wir mit der Detecon im vergangenen Jahr auf der Hannover-Messe mit einem IoT-Testcase aus Fischertechnik gezeigt. Als partnerschaftliches Projekt gemeinsam mit der Software AG entwickelt, haben die Berater hier einen dreistufigen IIoT-Architekturansatz realisiert, der damit genau der vom Industrial Internet Consortium vorgeschlagenen und beschriebenen Referenzarchitektur entspricht.

Informationsarchitektur ermöglicht Edge-Szenarien

Konkret bildet die zugrundeliegende Informationsarchitektur drei Ebenen ab:

- Edge-Ebene, deren Edge Gateway samt Senso-

ren und Aktoren sich direkt am Produkt oder einer Fertigungsinsel befinden

- Plattform-Ebene, die die Informations- und Ausführungssysteme (etwa für eine gesamte Fabrikanlage) umfasst
- Unternehmensebene, die die Geschäftsapplikationen in der Cloud beinhaltet.

Mit einem solchen Implementierungsbeispiel lassen sich Szenarien sowohl für die Fertigungssteuerung mit intelligenten Bauteilen als auch Predictive Maintenance darstellen.

Da der Edge Controller sich hier möglichst nah bei den jeweiligen Gerätesensoren befindet, kann er intelligent steuern, welche (in der Regel besonders latenzkritischen) Sensordaten direkt am Endgerät, also etwa einer einzelnen Fertigungsstation weiterverarbeitet werden müssen. Andere Daten wiederum schickt er aggregiert weiter in die Cloud für weniger zeitkritische Anwendungen. Wieder andere – eher unkritische Daten – werden überhaupt nicht ausgelesen, was damit auch insgesamt die Leitungskapazitäten schont.

Somit wird es möglich, bestimmte Ereignistypen in der Produktion je nach Kritikalität unterschiedlich schnell zu bearbeiten. Bevor ein Fräskopf gegen die Wand fährt, muss direkt an der Anlage direkt reagiert werden, während andere Informationen wiederum übergreifend der ganzen Fabrik mitzuteilen sind, weil sonst der Anlagentakt gefährdet wäre.

Netzarchitektur individuell am Use Case ausrichten

Die tatsächliche Ausgestaltung im realen Einsatz muss immer abhängig von den jeweilig gewünschten Use Cases variieren. Es ist immer eine Architekturentscheidung, ob die Latenz eher im Netzwerk, an einer Fertigungsstation oder in einem Fahrzeug verortet werden soll. Die Entscheidung orientiert sich zumeist an möglichst auszuschließenden Sicherheitsrisiken, aber auch an den Kosteneinsparungen eines effizienteren Datenaushalts, an gewünschten Analysemöglichkeiten für neue Geschäftsmodelle wie auch nicht zuletzt an den physikalischen Gegebenheiten.

Die Fischertechnik-Fabrik demonstriert all diese Zusammenhänge in realistischen Abläufen: Kleine Fahrzeuge steuern eine Anlagestation an, der Greifer meldet Vollzug, nachdem ein Gerät verschraubt und mit einem Tag versehen ist. Besonders wichtig: Die Rückmeldungsinformationen werden sofort verarbeitet, damit das Flurfahrzeug weiß, welche Station es ansteuern kann, wenn eine bestimmte Station gerade belegt ist. Ebenso melden Tags fortlaufend Informationen wie Energieverbrauch, Geschwindigkeit und Temperatur an die Steuerungsplanung zurück.

Informationsrückfluss steigert Planungsqualität

Besonders wertvoll ist, dass Daten in beide Richtungen und in Echtzeit zwischen Entwicklung, Planung und Produktion laufen. Gerade dies ermöglicht erst, dass Ablauf- oder Qualitätsänderungen berücksichtigt oder auch bewusst zu einem späteren Zeitpunkt noch mit vertretbarem Aufwand einzubringen sind. Diese mitunter riesigen Datenmengen und Informationen sind aber nicht alle gleichermaßen relevant für die Planung. Umgekehrt sind nicht alle Planungsdaten in der laufenden Produktion nötig. Die Herausforderung besteht darin, allen wirklich nutzgerechte Informationen am richtigen Ort und zur richtigen Zeit zur Verfügung zu stellen.

Hierfür sei neben der erforderlichen Business Intelligence vor allem auch ein möglichst semantisch einheitliches und übergreifendes Informationsmodell für den durchgängigen Datenfluss erforderlich. Hinzu kommt die technische Interoperabilität aller Komponenten der Plattform, wobei Modularisierung und Standardisierung eine wichtige Rolle spielen. Erfolgsentscheidend ist für alle Beteiligten zudem immer, sich vorher möglichst genau mit den fachlichen Zielen auseinanderzusetzen und die erforderlichen Tools nicht nur zum IoT-Selbstzweck einzusetzen.

Uwe Weber

Die flächendeckende Anwendung von IoT-Geräten in Industrie-Unternehmen – eine Bestandsaufnahme aus Sicht der Rückversicherung

WannaCry war im Mai 2017 ein vielbeachtetes Thema in der weltweiten Presse: Die Ransomware hatte über 200.000 Computer in 150 Ländern infiziert und jeweils Lösegeldzahlungen verlangt. Das Ereignis gilt als Weckruf gegen den sorglosen Umgang mit IT-Sicherheit. Die Schadsoftware Mirai machte im Oktober 2016 großflächig IoT-Geräte zu „Zombies“ und erzeugte ein Botnet, das u.a. DDoS-Angriffe gegen Firmen wie Dyn durchführte. Infolge dieses Angriffs waren Websites wie Twitter, Amazon oder Spotify zeitweise unerreichbar. Dieselbe Schadsoftware war auch für den stundenlangen Ausfall von 900.000 Telekom Routern in Deutschland verantwortlich.

Die erheblichen Potentiale, die sich aus den vernetzten, smarten Geräten ergeben, scheinen offensichtlich. Doch welchen Herausforderungen ist der industrielle Bereich im Kontext Internet of things ausgesetzt?

Munich Re Experten analysieren IoT-bedingte Schadensszenarien

Bei vielen IoT-Geräten spielt Sicherheit derzeit nur eine untergeordnete Rolle, sowohl im Design

und in der Entwicklung, als auch während des Produktlebenszyklus. Dies führt zu Sicherheitslücken, die häufig automatisiert und großflächig ausgebeutet werden können. In einem interdisziplinären Experten-Workshop hat Munich Re Ende 2017 anhand von Risikoszenarien IoT-bedingte Bedrohungen und Konsequenzen für Industrieunternehmen analysiert. Dabei hatte man sich auf die Risikomanagement-Methodik ISO 27005 gestützt und für die Abschätzung der Risiken die Automobilbranche und kritische Energie-Infrastrukturen als konkrete Beispiele verwendet.

Beispiel Automobilherstellung - vom Internet zum Intranet

Im industriellen Bereich bietet sich die Automobilherstellung als nachvollziehbares Muster für die Analyse der sogenannten smart factory an. In Deutschland sind rund zwei Millionen Menschen direkt oder indirekt in der Autoindustrie beschäftigt. Bei großen Automobilherstellern sind schon heute weit über 100.000 IoT-Geräte, vor allem Messgeräte, in der Produktion miteinander vernetzt. Tendenz: stark steigend.

Industrielle Steueranlagen, einzelne Sensoren und Aktoren sind Ziele, welche die Exponierung für Cyber Angriffe erhöhen. Bei einem französischen Autoproduzenten sorgte WannaCry für tagelangen Stillstand in mehreren großen Werken. Ein deutscher Automobilhersteller wird laut eigener Aussage etwa 6.000 Cyber-Angriffen pro Woche ausgesetzt. Dies sind meist vergleichsweise harmlose Versuche automatisierter Systeme oder Spielereien Computer-begeisterter Jugendlicher („Script Kiddies“), die aber die Dringlichkeit guter und aktueller Sicherheitssysteme verdeutlichen. Ferner ist davon auszugehen, dass die Häufigkeit der IoT-bedingten Schäden zwar langfristig abnimmt, aber kurz- und mittelfristig sogar zunimmt, weil es wesentlich mehr miteinander vernetzte IoT-Geräte gibt. Dazu kommt: Wenn ein Cyber-Angriff, etwa durch gezieltes Hacken und Manipulieren von Steuerungssoftware, gelingt, ist der Impact für die intelligente Fabrik erheblich. Gerade im Automobilbereich besteht in Ländern wie Deutschland ein Klumpenrisiko, weil entscheidende, voneinander abhängige Produktionsschritte durch unachtsamen Einsatz von IoT-Geräten gewichtigen Cyber-Gefahren ausgesetzt sind. Aufgrund der systemischen Verknüpfung sind Domino-Effekte in den Lieferketten vorstellbar, die einen ganzen Industrie-Zweig erfassen können.

Die großen Autobauer haben diese Problematik erkannt und schotten ihre IT stark von äußeren Zugängen ab. Da die Vernetzung aus Sicherheitsgründen vor allem nach innen gerichtet ist, spricht man in diesem Zusammenhang nicht vom Internet



Tim Kappler, Spezialist für Haftpflicht, Munich Re



Uwe Weber, Managing Partner und Leiter, Detecon Digital Engineering Center

sondern vom Intranet of Things. Die spannende Frage bleibt: Wie steht es um die Sicherheit der kleinen und mittelständischen Betriebe? Das Bild ist heterogen: Je nach Aufwand ist die Sicherheitsarchitektur stabil oder leicht angreifbar. IT-Manager und Sicherheitsarchitekten müssen Themen wie Zugriffskontrolle, Patch-Management und Netzwerkarchitektur auditieren und im Rahmen des Business Continuity Managements sicherstellen, dass auch für IoT-bedingte Betriebsunterbrechungen Notfallpläne bereit liegen. Zukünftig wird es darüber hinaus auch nützlich sein, IT-Sicherheit gegenüber möglichen Kunden mittels Zertifizierung (z.B. ISO 27001) zu belegen. Haftpflicht- und Sachversicherungen werden zunehmend durch Cyber-Versicherungen ergänzt, damit Cyber-Zwischenfälle nicht die Existenz eines Unternehmens gefährden.

Beispiel kritische Energie-Infrastruktur - wenn Windräder verrücktspielen

Bei der Analyse möglicher Schadensszenarien aus dem Bereich der Energie-Infrastruktur hat man sich auf Kraftwerks- und Gerätearten fokussiert, bei denen bereits heute eine ausgeprägte Vernetzung mittels IoT-Geräten festzustellen ist. Gerade in der Energiewirtschaft sind Sensoren nicht neu: Fernwartung und Fernsteuerung sind beispielsweise bei Windparks schon seit Jahrzehnten üblich und auch nötig. Es würde schlichtweg zu lange dauern, für jedes Softwareupdate auf jedes einzelne Windrad zu klettern. Das heißt konkret: Auf Messgeräte und die Steuerung kann über das Internet zugegriffen werden.

Auch in diesem Bereich haben die Analysen Einfallstore für Malware und gezielte Manipulationen zu Tage gefördert. Zwei Beispiele: In einem der Szenarien gelingt es Hackern, Windturbinen zu paralysieren. Hier geht es den Hackern darum, den Zugriff erst nach Zahlung eines Lösegelds wieder frei zu geben. In einem anderen Szenario übernehmen Hacker mittels Trojaner-Programm die Steuerung eines Windparks und stellen die Windkraftblätter in extrem starken Wind, sodass die Rotorblätter heiß laufen und die Gondel Feuer fängt. Im worst case reißen die Rotorblätter ab. Für einen Offshore-Windpark mit 50 bis 100 beschädigten Windkraftträgern wäre dies ein Sachschaden und damit einhergehend ein Betriebsunterbrechungsschaden in Millionenhöhe.

IoT im industriellen Einsatz - Positive Effekte im Überblick

- Bei allen oben beschriebenen Gefahren darf nicht vergessen werden, dass der Einsatz von vernetzten Geräten viele Vorteile bringt. Zum Beispiel sind heutige Kameras deutlich besser als das menschliche Auge, sie können Fehler erken-

nen, die der Mensch nur unter dem Mikroskop sehen würde und das 1000 Mal in der Zeit eines Wimpernschlags.

- Die Produktionsqualität wird sich mittelfristig erhöhen, Fehler aus menschlichem Verhalten werden abnehmen. Produkt-Rückrufe werden einfacher und schneller durchzuführen sein.
- Die Vernetzung von Messgeräten wird den Fernzugriff auf schwer zugängliche Maschinen vereinfachen.
- Zuverlässige Vorhersagen über den Zustand von Maschinen und erforderliche Wartungsperioden ("predictive maintenance") werden durch Nutzung von IoT-Daten möglich. Maschinenbruch und Betriebsunterbrechungen sind dadurch langfristig rückläufig.

IoT im industriellen Einsatz - Negative Effekte im Überblick

- Die Anzahl der Sicherheitslücken nimmt mit jedem weiteren IoT-Gerät zu.
- Es ist mit einer steigenden Zahl von Angreifern und Angriffen zu rechnen.
- Cyber-Schwachstellen in IoT-Geräten können nicht nur zu Vermögensschäden, sondern auch zu physischen Schäden führen.
- Trotz steigender Anforderungen an Wartung und Aktualisierung der IT wird die Anzahl der IT-Mitarbeiter mit dem rasanten Zuwachs von IoT-Geräten kaum Schritt halten können.

Fazit

Schäden in einer voll vernetzten Industrie werden langfristig seltener auftreten; sollte es jedoch zu Schäden kommen, werden diese höher ausfallen und eine Vielzahl von Industrieunternehmen treffen, beispielsweise, weil ganze Industriezweige die gleiche Software oder die gleichen IoT-Geräte verwenden. Man spricht hierbei von Kumul-Fällen. Beim Einsatz von IoT-Geräten in der smart factory ist ein genaues Verständnis von technischen Abhängigkeiten nötig und die regelmäßige Auditierung hinsichtlich möglicher Schwachstellen durch unabhängige Spezialisten empfehlenswert.

Da es 100% Sicherheit nicht geben kann, ist es ratsam, die verbleibenden Restrisiken über Versicherungslösungen abzutragen. Aufgrund der hohen Komplexität sind maßgeschneiderte, spartenübergreifende Lösungen für Produkthaftpflichtrisiken, Betriebsunterbrechungen und Reputationsschäden durch schadhafte Software oder Cyberattacken erforderlich. Munich Re leistet als Rückversicherer hierzu einen wertvollen Beitrag.

Tim Kappler

Nutzen Sie Storytelling – die fünf Storys, die jeder braucht



Es egal ob Sie in den ICE steigen und ein Gespräch mit dem Sitznachbarn beginnen. Ob Sie auf einer Party zu einer Gästerunde stoßen, in der Sie niemanden kennen. Oder ob jemand das erste Mal auf Ihrer Firmenwebsite landet und nichts über Ihr Unternehmen weiß. Viele Situationen im täglichen Leben führen dazu, dass Sie sich vorstellen müssen.

Um sich in diesen Momenten auf den Punkt zu erzählen, sollten Sie folgende Storyarten kennen und ausformulieren.

1. Die „Was wir tun“-Geschichte: (Nutzensgeschichte)

Erzählen Sie anhand einer bildhaften Geschichte genau, was Sie tun. Nicht nur: „Ich arbeite in einer IT-Abteilung.“ Seien Sie spezifisch. „Ich bin der Projektleiter für ein 40-Mann-Team in der IT-Security. Ein bisschen ist das, wie in der Abteilung eines Geheimdienstes, der Jagd auf die eigene Regierung macht, um Schwachstellen im System zu finden. Aber so war das schon immer – ich liebe Krimis und finde es spannend zu tüfteln.“ Schon hinterlassen Sie einen persönlichen Eindruck und eine Erinnerung.

2. Die „Wie kommen wir dazu“-Geschichte: (Entstehungsgeschichte)

Menschen wollen wissen, wie wir zu dem gekommen sind, was wir heute tun. Genau dieses „Warum“ macht oft den Unterschied und bildet Vertrauenskapital, das dann eine Zusammenarbeit ermöglicht. Schreiben Sie nicht nur: „Ich bin seit 2002 Ingenieur.“ Sondern schreiben Sie darüber, wie sehr Sie Ihren Großvater bewundert haben. Der war Ingenieur und hat mit Ihnen auf dem Schoß aus seiner Amateurfuncker-Werkstatt im Pazifik angerufen. Von ihm haben Sie die Begeisterung für technische Möglichkeiten geerbt.

3. Die „Wofür wir stehen“-Geschichte: (Differenzierungsgeschichte)

Menschen interessieren sich dafür, wie wir etwas machen. Was unterscheidet uns von anderen? Was macht uns einzigartig und wertvoll? Wenn Sie Bäcker sind, erzählen Sie, wie genau Sie Ihre Bäckerei betreiben. Ihren Kunden geht es nicht nur um süße und salzige Backwaren. Sie kommen zu Ihnen, weil Sie einen sozialen Marktplatz mit Atmosphäre

bieten, der Ihren Kunden beim Kaufen und Genießen einen Kurzurlaub vom Alltag ermöglicht. Deshalb haben Sie rund um die Bäckertheke ein gemütliches Strandcafé errichtet. Sofort merken Ihre Zuhörer: Hier ist ein Mensch am Werk, den eigene, besondere Werte antreiben.

4. Die „Was wir bewirken“-Geschichte: (Erfolgsgeschichte)

Nichts lässt uns mehr glänzen, als wenn wir unseren Nutzen über eine erfolgreiche Wirkung erzählen können. Erzählen Sie dazu eine konkrete Geschichte: Sie bekamen vom Vorstand den Auftrag, das größte Desaster des Konzerns zu sanieren. Den Fall kannten Sie bereits, denn den kannte jeder. Zuerst haben Sie das Gespräch mit den Führungskräften gesucht und sich überlegt, ob dieses Unternehmen noch wirkliche Marktchancen in der digitalen Welt hat. Lohnte es sich, dem Unternehmen bei der Gesundung zu helfen? Erzählen Sie szenisch, dann wollen Ihre Zuhörer auch wissen, wie die Geschichte ausgeht.

5. Die „Was Kunden über uns erzählen“-Geschichte (Kundengeschichte)

Wie schön ist es, wenn nicht Sie, sondern andere über Sie sprechen. Sei es im Vorstand, in einer Sitzung oder auf LinkedIn. Lassen Sie Ihre Kunden Ihre Erfolgsgeschichte erzählen. Das könnte so klingen: „Ich war immer skeptisch gegenüber Coaches. Doch als ich dann erlebt habe, wie aktiv Frau Meyerhold mir zugehört hat, wie sie in der Lage war, meine Situation genau zu verstehen, das hat mich echt begeistert. Die Lösung tauchte dann wie von selbst auf. Ich fühlte mich einfach gestärkt in meiner Wahrnehmung und auf meinem Weg. Ich konnte sofort meine Ziele wieder klar sehen und auch umsetzen. Die regelmäßigen Termine helfen mir, meine Kraft auf die Straße zu bringen.“ Bei solchen Aussagen haben mögliche Neukunden und Partner sofort Rückkopplungen. Sie können sich in der Story, dem Testimonial wiedererkennen. Ihre Meinungsbildung wird bis zur Entscheidungsreife gestärkt und gesättigt. Uwe Walter

Uwe Walter ist Storytelling- und Change-Experte für Medien- und Industrieunternehmen. Er berät so unterschiedliche Kunden wie YouTube-Stars, Start-ups, Blogger, Verlage, Radio- und Fernsehsender sowie Filmproduktionen. Seine Expertise: Wie generiere ich Reichweite durch zukunftsicheres Erzählen?

Den inhaltlichen Auftakt des Abends gibt dann Sven Hellman von der Firma Cassini mit einleitenden Worten zum Thema Smart City München.



Der erste Workshop der Smart City AG fand an der LMU München statt.



MÜNCHEN

Arbeitsgruppe Smart City München

Digitale Stadt München startet mit erster Arbeitsgruppe

Nachdem beim ersten Digitalk bei Cassini die Arbeitsgruppe Smart City ins Leben gerufen wurde, fand am 10. April der erste Workshop statt.

14 Personen aus verschiedenen Unternehmen nahmen daran teil und diskutierten in dieser ersten Runde über die Zielsetzung und die Roadmap für 2018. Zukünftig sollen die Arbeitsergebnisse der AG auch einen Platz auf der Website des Digitale Stadt München e. V. finden.

MÜNCHEN

Digitale Stadt München e. V.

Digitalk bei Cassini

Nach einigen einführenden Worten der Vorsitzenden der Digitalen Stadt München, Prof. Dr. Linnhoff-Popien, zu dem höchst erfolgreichen Mitgliederzuwachs des Vereins – aktuell sind es 91 Mitglieder – stellte die Vorsitzende die neuen Arbeitsgruppen vor, bei welchen jedes Mitglied sich inhaltlich einbringen kann. Der Pilotversuch ist – passend zum Digitalk – das Thema Smart City. Der Abend wurde mit einem Vortrag von Cassini zum Thema Smart City eröffnet. Bernhard Klassen von der Landeshauptstadt München stellte daraufhin das Münchner Leuchtturmprojekt „Smarter-Together“ vor. In diesem von der EU geförderten Projekt versuchen die Städte München, Lyon und Wien gemeinsam Smart-City-Lösungen zu entwickeln und zu testen. Abschließend sprach Michael Zaddach – CIO des Flughafens München – über Smart City in Bezug auf den Airport, da dieser selbst wie eine kleine Stadt funktioniert. Im Anschluss fand bei einem kunstvoll angerichteten Catering und kühlen Getränken Networking statt. Auch konnten sich die Gäste in vorbereiteten Topic-Corners zu den Themen Blockchain und Situational Awareness informieren.



Den inhaltlichen Schlusspunkt setzt Michael Zaddach vom Flughafen München und erklärt, was „Smart“ im Kontext des Flughafens bedeutet und welche Schwierigkeiten sich dabei ergeben.



Im Anschluss gibt es noch feine Häppchen.

Etwa 70 Teilnehmer waren gekommen, um den verschiedenen Vorträgen zum Thema „Smart City München“ zuzuhören.



Otto Lindner, Vorstand der Lindner Hotels AG, im Gespräch mit Stephan Schneider, Vorstandsvorsitzender des Digitale Stadt Düsseldorf e.V.



V. l. n. r.: Prof. Christian Börsing (Campusmanager EMBA Düsseldorf), Thomas Dittrich (EMBA-Geschäftsführer), Stephan Schneider (Vorstandsvorsitzender Digitale Stadt Düsseldorf) und Sebastian Milbrandt (zweiter EMBA-Geschäftsführer).

DÜSSELDORF

Digitale Stadt Düsseldorf e. V.

Beim ersten Digitalk der Digitalen Stadt Düsseldorf in diesem Jahr stand Cybercrime im Fokus. Der Vortrag von Markus Hartmann, Oberstaatsanwalt bei der Staatsanwaltschaft Köln und Leiter der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW), gab einen Überblick über die aktuelle unternehmensbezogene Bedrohungslage und zeigte auf, welchen Beitrag die Justiz Nordrhein-Westfalens zu einer gemeinsamen Cybersicherheitsstrategie leistet.

Der nächste Digitalk in Düsseldorf fand dann bei der Europäischen Medien- und Business-Akademie (EMBA) statt. Digitaler Wandel, Industrie 4.0, Big Data, Internet der Dinge und mobile Vernetzung sind nur einige Stichworte für den ebenso rasanten wie nachhaltigen Wandel aller Wirtschafts- und Lebensbereiche durch Daten und Digitalisierung. Die EMBA hat – umfragegestützt auf die konkret gewünschten Berufsprofile der Digitalwirtschaft – mit ihrem Studiengang „Digital Business Management“ dafür ein neues innovatives Studienangebot entwickelt. Der neue Düsseldorfer Campus-Manager der EMBA, Prof. Christian Börsing, und zweiter EMBA-Geschäftsführer Sebastian Milbrandt stellten den zukunftsorientierten Studiengang mit seinen verschiedenen Studienrichtungen auf dem Digitalk der Digitalen Stadt Düsseldorf vor.

Mehr als 200 Teilnehmer kamen zum ersten Digitalk des Jahres in das Lindner Congress Hotel.



Nach dem Vortrag zu „Cybercrime und Cyberkrise“ wurde der Abend in lockeren Gesprächen beendet.

LEIPZIG

XPOMET© 2018

Die XPOMET© Convention für Innovation und Hightech in der Medizin feierte in der letzten Woche ihr dreitägiges Debüt mit großem Erfolg und Begeisterung aller Beteiligten.

Auf die in der zweijährigen Vorbereitungsphase zur Veranstaltung immer wieder aufgetauchten Skepsis der Branche, ob es denn noch ein weiteres Healthcare-Event auf dem Markt bräuchte, kann zur Freude des XPOMET© Teams nun ein klares „Ja“ entgegengebracht werden:

Mit einem unkonventionellen und innovativen Format schaffte es die XPOMET©, eine mannigfaltige, inspirierte Masse an vorwärtsdenkenden Playern des gesamten Gesundheitswesens vor Ort zu versammeln und in eine neue Art von Diskurs und Austausch zu involvieren. Nach der feierlichen Eröffnung durch die sächsische Staatsministerin Klepsch und den Pepper-Roboter Max (FH Kiel) bot sich den Teilnehmern ein volles Programm mit insgesamt 153 internationalen Experten und Hochkarättern auf den Bühnen sowie zahlreichen Think Tanks und hands-on Use-Case-Sessions, die dabei für ein interaktives Setting sorgten, in dem es keinen Platz für Langeweile gab. Lernen, erleben, ausprobieren und gemeinsam schneller voranschreiten, um zu ändern und zu verbessern - das war der Spirit, von dem sich in der Leipziger Kongresshalle in den drei Tagen insgesamt über 1.600 Teilnehmer anstecken ließen. Der „XPOMET Spirit“ wurde nicht zuletzt von den Pionieren der neuen Healthcare Era wie Nick Adkins oder Joao Bocas geprägt, die alle Beteiligten mit dem internationalen #pinksocks Movement und ihrem ansteckenden Enthusiasmus packten - ein solches Community-Gefühl dürfte es wohl auf noch keiner europäischen Healthcare-Veranstaltung gegeben haben. Doch nicht nur hier wurden die Erwartungen des Organisationsteams um Ulrich Pieper (Gründer), Josefine Hofmann (Convention & Program Director) und Lena Geppert (Geschäftsleitung VdigG e.V./Co-Host) weit übertroffen: „Thank you all for creating this amazing platform and bringing together such a diverse crowd! Well done!“ Bart de Witte, Director of Digital Health DACH IBM



Nick Adkins beschreibt seine Entwicklung vom Healthcare Executive zum Kilt-tragenden Digital Health Evangelisten.



Die Pink-Socks-Bewegung rund um Nick Adkins vereint auch auf der XPOMET© unterschiedliche Akteure im Healthcare-Bereich.



Die neuen Formate wie der Showcase „Notaufnahme der Zukunft“ sind nicht die Einzigen, die die Vereinfachung der Abläufe in der Zukunft zeigen sollen.



Unterschiedliche Aussteller vom Start-up bis zu großen Playern stellen ihre Innovationen vor.

Die zwei Ausstellungsflächen sind nach unterschiedlichen Themenbereichen unterteilt.

Fotos: Xpomet

FACHBEIRAT



Robert Blackburn
CEO Hoffmann Group



Patric Fedlmeier
CIO Provinzial Rheinland



Norbert Gaus
Executive VP SIEMENS



Sandro Gaycken
Direktor ESMT



Michaela Harlander
Vorstand Harlander-Stiftung



Markus Heyn
GF BOSCH



Martin Hofmann
CIO Volkswagen



Manfred Klaus
Sprecher der GF Plan.Net



Andrea Martin
CTO IBM



Niko Mohr
Partner McKinsey



Frank Rosenberger
Group Director TUI



Joachim Schäfer
GF Messe Düsseldorf



Ralf Schneider
CIO Allianz Group



Stephan Schneider
Manager Vodafone



Marc Schröder
GL MG RTL Deutschland



Uwe Walter
Waltermedia



Michael Zaddach
CIO Flughafen München

INFO FÜR UNSERE LESER UND ABONNENTEN:

Zum Juni 2018 haben wir den Verlag gewechselt. Die **DIGITALE WELT** wird nun von der Vogel Business Media GmbH & Co. KG verlegt. In diesem Zusammenhang hat sich eine Anpassung des Bezugspreises ergeben. Unser Magazin erhalten Sie in der gewohnten Regelmäßigkeit weiterhin im Abo.

Wir bedanken uns sehr herzlich bei der eMedia Gesellschaft für elektronische Medien mbH für die mehrjährige vertrauensvolle Zusammenarbeit.

IMPRESSUM

VERLAG

Vogel Business Media GmbH & Co. KG, Max-Planck-Str. 7/9, 97064 Würzburg, www.vogel.de

Geschäftsführer

Matthias Bauer, Florian Fischer, Günter Schürger

REDAKTION

Chefredaktion Claudia Linnhoff-Popien (V. i. S. d. P.)

Chef vom Dienst Marie Kiermeier

Fachbeirat Robert Blackburn, Patric Fedlmeier, Norbert Gaus, Sandro Gaycken, Michaela Harlander, Markus Heyn, Martin Hofmann, Manfred Klaus, Andrea Martin, Niko Mohr, Frank Rosenberger, Joachim Schäfer, Ralf Schneider, Stephan Schneider, Marc Schröder, Uwe Walter, Michael Zaddach

Redaktion Florentina Hofbauer

Blog Steffen Illium

Redaktionsassistenten Kerstin Fischer, Katja Grenner, Tanja Zecca

Mitarbeiter dieser Ausgabe Sebastian Feld, Thomas Gabor, Kyryll Schmid, Andreas Sedlmeier, Lorenz Schauer

Schlussredaktion KorrekturService Sand, Wolfgang Sand, Ahornallee 89, 86899 Landsberg

ANFRAGEN AN DIE REDAKTION

redaktion@digitaleweltmagazin.de

GRAFIK

Layout Stefan Stockinger, www.stefanstockinger.com

ANZEIGEN

Vogel Corporate Media GmbH, Leipziger Straße 126, 10117 Berlin

Ansprechpartner Bianca Welsch, Tel. +49 30 890 48-1221, E-Mail: bianca.welsch@vogel-corporatemedie.de

Es gilt die gültige Preisliste, Informationen hierzu unter www.digitaleweltmagazin.de/mediadaten

HERSTELLUNG

ColorDruck Solutions GmbH, Gutenbergstraße 4, 69181 Leimen

ABO-SERVICE

DataM-Services GmbH, Aboservice Digitale Welt, Franz-Horn-Str. 2, 97082 Würzburg, Tel. +49 931 4170-435

E-Mail: abodigitalewelt@vogel.de

Digitale Welt erscheint einmal pro Quartal

ABONNEMENT-PREISE

Jahres-Abo inklusive Versandkosten: Inland 78,00 €, Ausland 87,60 €; ermäßigtes Abo für Schüler, Studenten, Auszubildende: Inland 39,00 €

Der Bezug der Zeitschrift Digitale Welt ist im Mitgliedsbeitrag des Verbandes VOICE – Bundesverband der IT-Anwender e. V., Digitale Stadt München e. V. und Hannover IT e. V. enthalten.

HERAUSGEBER

Prof. Dr. Claudia Linnhoff-Popien, Institut für Informatik, Ludwig-Maximilians-Universität München, Oettingenstr. 67, 80538 München, Tel. +49 89 2180-9153, www.digitaleweltmagazin.de

RECHTE

Dieses Magazin und alle in ihm enthaltenen Beiträge, Abbildungen, Entwürfe und Pläne sowie Darstellungen von Ideen sind urheberrechtlich geschützt. Mit Ausnahme der gesetzlich zugelassenen Fälle ist eine Verwertung einschließlich Nachdrucks ohne schriftliche Einwilligung des Herausgebers strafbar. Für unverlangt eingesandte Manuskripte und Bildmaterial übernehmen Redaktion und Verlag keine Haftung.

CALL FOR CONTRIBUTION

für den DIGITALE-WELT-Blog



Die nächste
DIGITALE WELT
erscheint am
05.09.2018

Werden Sie Teil unserer hochkarätigen Autorenschaft und platzieren Sie Ihre Digitalthemen von morgen auf der Plattform von heute mit bislang **147.000*** Klicks.

UNSERE NÄCHSTEN
SCHWERPUNKTTHEMEN IM ÜBERBLICK

- ✓ **Machine Learning (IV/18)**
- ✓ **Data Science / Data Mining (I/19)**

WEITERE THEMEN-SPECIALS:

- ✓ **Quantencomputing**
- ✓ **Reinforcement Learning**

INTERESSE GEWECKT?

Dann melden Sie sich bei der **DIGITALE WELT** -Redaktion per E-Mail: blog@digitaletweltmagazin.de oder telefonisch unter der +49 89 2180 9171.

*Unsere Beiträge wurden online unter www.digitaletweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 1. August 2017 – 2. Mai 2018.

Termine

INNOVATION JOURNEY @ AUTOMATICA

Termin: 20.–21. Juni 2018 | Ort: Messe München

Begeben Sie sich mit Führungskräften anderer Unternehmen auf eine Expertenreise, die sich diesmal insbesondere der Fragestellung widmet, wie zukünftig innovative Produkte entwickelt werden und welche ethischen Fragestellungen dabei zu beachten sind. Und welche Branche würde hier aktuell spannendere Einblicke geben als die Welt der Robotik? Wir besuchen Innovationslabore von Start-ups und globalen Playern – von Medineering bis IBM Watson. Wir treffen die Vordenker aus Praxis und Wissenschaft, wie u. a. den renommierten Professor Sami Haddadin. Wir diskutieren mit Experten der Branche in exklusivem Kreis auf einer der weltgrößten Robotik-Messen, der automatica. Und wir bauen sogar selbst einen Roboter mit Franka Emika. Melden Sie sich jetzt per E-Mail an mail@innovationjourney.net an und seien Sie dabei, wenn es heißt „Embrace the robots!“

PLAY VIDEO SUMMIT

Termin: 18. Oktober 2018 | Ort: Hamburg

Der PLAY Summit zeigt das gesamte Spektrum von Video-Marketing in klassischen und digitalen Umfeldern. TV-Spots und die Möglichkeiten ihrer Verbreitung sind ebenso Thema wie rein digitale Konzepte für Onlinemedien und Social-Plattformen. Kreation, Channels, Technologie und Audience sind die Leitthemen, die in Vorträgen, Cases und Diskussionen inhaltlich verknüpft werden. Um den PLAY SUMMIT 2018 einzuläuten, präsentieren Speaker nationaler Top-Brands und Bereichsexperten richtungweisende Entwicklungen in der Bewegtbild-Werbung für TV, Mobile, Website und soziale Plattformen wie YouTube, Facebook & Co. Im anschließenden Diskussions- und Networking-Exchange haben Sie die Chance, sich mit den Größen der digitalen

Szene auszutauschen, neue Ideen zu entwickeln und innovative Ansätze für Ihre Strategien mit den Marketing-Technologien der Zukunft zu erkunden. Das Programm und weitere Informationen finden Sie unter: <https://play-summit.com/>

NEW MARKETING TECH SUMMIT

Termin: 7. November 2018 | Ort: Hamburg

Neue Wege und Strategien im Marketing sind untrennbar mit Technologie verbunden, Unternehmen müssen die Optionen kennen, zu denen Data und Technologie sie im Umgang mit Kunden befähigen. Der NEW MARKETING TECH SUMMIT präsentiert die neuesten Ansätze, die schlauesten Köpfe und die innovativsten Technologien. Wir arbeiten derzeit mit Hochdruck an der Agenda. Weitere Informationen über das geplante Programm und die auftretenden Speaker unter: <https://conference.newmarketing.de/>

DIGICON 2018

Termin: 21.–22. November 2018 | Ort: Palais Lenbach, München

Auf der DIGICON 2018 erwarten wir mehr als 400 Top-Entscheider aus über 150 Firmen wie Allianz, BOSCH, Flughafen München, Generali, Google, HypoVereinsbank, LMU München, Münchner Rück, Siemens, Pro7Sat1, Vodafone, Wacker Chemie u. v. a. m. Internationale Experten aus Wirtschaft und Wissenschaft stellen den Teilnehmern neueste Trends, Entwicklungen und Ergebnisse rund um das Thema Machine Learning vor. Anwender referieren über Success Storys, Analysten über die Methoden dahinter.

Nutzen Sie die Gelegenheit, sich auszutauschen, und betrachten Sie neueste, bahnbrechende Entwicklungen zum Machine Learning aus Perspektiven wie Quantencomputing, Data Mining und Reinforcement Learning.

Der Status quo ist der Hintern. Du bist der Tritt.

Next Digital Leader gesucht! Du willst etwas bewegen und kannst auch mal unbequem sein? Dann bist du bei uns genau richtig. Egal, ob du noch studierst oder bereits im Beruf stehst – mit deinem Drang zur Digitalisierung machst du mit uns die deutsche Wirtschaft fit für die digitale Zukunft.

Interesse? Mehr auf next-digital-leader.de/



digital done differently



ProSiebenSat.1
Media SE



**CONNECT.
CODE.
CREATE.**

Are you curious?

Discover more at tech.prosiebensat1.com and explore our way of working and the fascinating people behind the scenes.